UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	CASE NO. CR19-00159-RSL
	)	
v.	)	Seattle, Washington
	)	
PAIGE A. THOMPSON,	)	June 8, 2022
	)	9:12 a.m.
Defendant.	)	
	)	JURY TRIAL, Vol. 2 of 9

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE ROBERT S. LASNIK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:

MOHAMMAD ALI HAMOUDI
NANCY TENNEY
Federal Public Defender's Office
1601 5th Avenue, Suite 700
Seattle, WA 90071

BRIAN E. KLEIN
MELISSA A. MEISTER
Waymaker LLP
515 S Flower Street, Suite 3500
Los Angeles, CA 90071

Reported by:

Nancy Bauer and Marci Chatelain
Official Federal Court Reporters
700 Stewart Street, Suite 17205
Seattle, WA 98101

INDEX

EXAMINATION OF		PAGE
STEVE SCHUSTER	DIRECT EXAMINATION BY MR. FRIEDMAN	62
	CROSS-EXAMINATION BY MR. KLEIN	118
	REDIRECT EXAMINATION BY MR. FRIEDMAN	137
KRISTEN VALENTINE	DIRECT EXAMINATION BY MS. MANCA	143
	CROSS-EXAMINATION BY MR. HAMOUDI	168
	REDIRECT EXAMINATION BY MS. MANCA	178
	RECROSS-EXAMINATION BY MR. HAMOUDI	178
MICHAEL FISK	DIRECT EXAMINATION BY MR. FRIEDMAN	179

GOVERNMENT'S OPENING STATEMENT BY MS. MANCA 20
DEFENSE'S OPENING STATEMENT BY MR. KLEIN 46

GOVERNMENT EXHIBITS

EXHIBIT	ADMITTED	WITHDRAWN
101	66	
102 THROUGH 110	68	
103	72	
104	75	
105	79	
106	84	
107	96	
108	98	
201	149	
202	149	
203	149	
204	149	
209	149	
913	71	
952	108	
954	106	

DEFENSE EXHIBITS

EXHIBITS	ADMITTED	WITHDRAWN
1010	173	
1011	174	

PROCEEDINGS

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE CLERK: United States District Court for the Western District of Washington is now in session, the Honorable Robert S. Lasnik presiding.

THE COURT: Good morning. Thanks. Please be seated.

THE CLERK: This is the matter of the United States versus Paige Thompson, cause number CR19-159, assigned to this Court.

If counsel could please rise and make your appearances.

MR. FRIEDMAN: Good morning, Your Honor. Andrew Friedman, Jessica Manca, and Tania Culbertson for the United States.

THE COURT: Thank you.

MR. HAMOUDI: Good morning, Your Honor, Mo Hamoudi, Brian Klein, Stacey Brownstein, Nancy Tenney, Emily Stierwalt, and Melissa Meister on behalf of Ms. Thompson.

THE COURT: Okay. Thank you very much.

We won't do this every day, but first day of the trial we're going to do this.

Okay. Let me just ask, Mr. Friedman, Count 3?

MR. FRIEDMAN: Your Honor, I'm sorry, we should have -- I think we had a footnote or something in one of the pleadings --

THE COURT: Yeah.

MR. FRIEDMAN: -- but, yeah, the -- based on our ability to get cooperation from an overseas victim, we would ask the Court to dismiss Count 3.

THE COURT: So the government's moved to dismiss Count 3, and I'll grant that motion.

MR. FRIEDMAN: Thank you, Your Honor.

THE COURT: Okay. So we now have 1, 2, 4 through 10.

MR. FRIEDMAN: Yes, Your Honor.

THE COURT: Okay. Great.

And I am going to read some of the advance instructions. I'm not going to go into a great deal of detail on the elements of the crimes, we're going to end up arguing about that and do that later. I'm just going to use the titles of the crime, and in the statement of the case, more of a generic kind of explanation of what's going on here.

So then, defense, Mr. Klein, do you have an objection to something that the government intends to do in opening?

MR. KLEIN: Yes, I do, Your Honor.

THE COURT: Tell me about that.

MR. KLEIN: Your Honor, I don't know if Your Honor has the slides with you.

THE COURT: I have the packet, yeah.

MR. KLEIN: Okay. And they're not numbered, so I'll just direct you to about 10 slides in with a slide that begins, server-side request forgery. There's three slides, that I can tell, dealing with that issue, Your Honor.

THE COURT: Server-side request forgery?

MR. KLEIN: Yes.

THE COURT: Okay. I got it.

MR. KLEIN: Your Honor, that's not the crime Ms. Thompson is charged with. And both Amazon, Capital One, and as far as we know every witness, will say that is not what happened here. She is charged with a proxy scanner attack.

And to introduce a crime that she's not charged with here in the opening, you know, we object. We find that, you know, objectionable for a number of reasons. But one is it will sow confusion. We understand Your Honor wants to allow in terms and explanations about what happened here so the jury can have a better understanding, but all this will do will sow confusion.

It's very clear, and Amazon has made it clear, as well as other witnesses whose discovery we read, that is not the attack that they're alleging. And so to talk about a very complex different type of attack will only create confusion for the juror [sic]. And we're worried that the jury might think she's committed something else, might get confused, ultimately make a decision or make -- go to a verdict on something that she didn't do, so we object.

THE COURT: Okay. And, Ms. Manca, you're not saying this is the name of a crime, but you are saying this is why Ms. Thompson was able to get in.

MS. MANCA: It's a commonly used method for an attack methodology. It's certainly not a crime.

We do have an expert witness in this case who will testify that this is a server-side request forgery. These slides are slides that he suggested, that's our forensic computer scientist, so we believe that this properly characterizes the evidence at trial.

THE COURT: Okay. It's opening statement. It's not evidence. It's not even closing argument. I'll allow it based on the government's representation that they have a witness, an expert witness, who will talk about it.

Anything else, Counsel?

MR. KLEIN: Nothing further, Your Honor.

THE COURT: Okay. Great.

And, Ms. Manca, approximately how long for opening?

MS. MANCA: I would say approximately 45 minutes.

THE COURT: Okay. And, Mr. Klein, approximately?

MR. KLEIN: Fifteen to 20 minutes, Your Honor.

THE COURT: Okay. Great. Appreciate that.

And again, I'm not going to put you on the clock or anything like that.

Okay. So we had a little trouble getting one of the jurors, but we have the full 15 now.

We'll have to come up with a better name than full 15 for them, but I can -- Victoria, you want to bring them on in?

And I'll just stay here, but we're in court at recess, okay?

So anybody wants to leave or walk around, it's okay. I just don't want to get off and come back again.

(Off the record.)

THE COURT: And then, Mr. Friedman, back on the record for a second, alleged victims, Capital One, Ohio Department of Public Safety, Michigan State University, Digital Ai, Bitglass, Enghouse Interactive, 42Lines?

MR. FRIEDMAN: Your Honor, those are the entities that are -- I think were numbered Victims 2, 3, 4, 5, 6, 7, and 8. There are not counts relating to all of those, for example, Ohio Department of Public Safety and Michigan State University. And there are other victims that will be mentioned.

I guess I should mention one other thing for the Court. Those were names -- or those were sometimes current names of the companies. There are a lot of acquisitions in this field. And so we've spoken with defense counsel about this, and Digital Ai is a current company -- I'm sorry, Enghouse is a current company. It acquired a company named Survox, and the data taken here was from Survox. And that will be sometimes referred to as Enghouse, sometimes as Survox. We'll try and make that clear.

Similarly, Digital Ai is a success- -- acquired a company named Apperian -- Arxan, which acquired a company named Apperian and this --

THE COURT REPORTER: I'm sorry. I'm sorry. Can you slow down a little bit?

THE COURT: Yeah, you lost me at Your Honor, so...

MR. FRIEDMAN: So Digital Ai acquired a company named Apperian, which -- I'm sorry, acquired a company named Arxan, which had acquired a company named Apperian. The data here is Apperian data from that segment of the business. And so that will often be referred to as Apperian. And I think, ultimately, the instructions will probably have both names in them.

THE COURT: Okay. Look, I'm -- you know, usually we read the names of people to see if anybody on the jury knows these people, but these things are so obscure, I'm not even going to go there.

But something like Michigan State University, somebody might have gone to Michigan State University or, you know, Ohio Department of Public Safety or something like that, but I don't need to know all these things, so...

MR. FRIEDMAN: Okay. Thank you Your Honor.

THE COURT: I might read some of them just to see if anybody has heard of the companies or anything like that, but I understand what you're saying, it's complicated.

MR. FRIEDMAN: Thanks.

MR. KLEIN: Your Honor, one more thing.

THE COURT: Yes, Mr. Klein.

MR. KLEIN: During my opening, I wanted to ask Ms. Thompson to stand up --

THE COURT: Sure.

MR. KLEIN: -- take off her mask and say hello to the to the jury, just so they can see her without her mask.

THE COURT: Absolutely. That's fine.

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: All right. Ladies and gentlemen of the jury, you are now the jury in this case. And I want to take a few minutes to tell you about your duties as jurors and give you some preliminary jury instructions. These I'm just going to read to you, and they're only preliminary.

At the end of the trial, right before closing argument, you will get a packet of written instructions for each juror that I will read to you, and that will go back into the jury room with you. And those are the ones that you will use to decide the case, but I'm giving you some advance oral instructions.

When you deliberate, it will be your duty to weigh and to evaluate all the evidence received in the case and in that process decide the facts. To the facts, as you find them, you will apply the law is I give it to you. And whether you agree with the law or not, you must decide the case solely on the evidence and the law that I give you.

You must perform these duties fairly and impartially. You should not be influenced by any person's race, color, religious beliefs, national ancestry, sexual orientation, gender identity, gender or economic circumstances. Do not allow yourselves to be influenced by personal likes or dislikes, sympathy, prejudice, fear, public opinion or biases, including unconscious biases.

Unconscious biases are stereotypes, attitudes or preferences that people may consciously reject, but may be expressed without conscious awareness, control or intention. Like conscious bias, unconscious bias can affect how we evaluate information and make decisions.

Now, this is a criminal case brought by the United States government. And the United States charges the defendant, Paige Thompson, with wire fraud, computer fraud and abuse, access device fraud, and aggravated identity theft.

The charges against the defendant are contained in an indictment. The indictment simply describes the charges that the government brings against the defendant.

The defendant has the right to remain silent and never has to prove innocence or present any evidence.

To help you follow the evidence, I will give you a brief summary of the elements of the crimes that the government must prove. And I'm not even going to go into the elements, I'm just going to give you an overview of the charges because it's going to be a difficult case to follow, and the lawyers and I have to work out the actual instructions that we'll give at the end of the case.

Count 1 charges the crime of wire fraud under 18, United States Code section 1343. This means that Ms. Thompson is accused of knowingly devising and intending to devise a scheme or plan to defraud or a scheme or plan for obtaining money or property from one who is deceived by means of false or fraudulent pretenses, representations, or promises, and using or causing to be used in interstate or foreign wire communication to carry out or attempt to carry out an essential part of the scheme.

Ms. Thompson is accused of doing this with intent to defraud, that is intent to deceive and cheat. And the statements made as part of the scheme are alleged to have been material.

Counts 2, 4, 5, 6, 7 and 8 arise under the Computer Fraud and Abuse Act, 18, United States Code, section 1030.

Counts 2, 4, 5, 6, and 7 charge Ms. Thompson with unlawfully obtaining information.

Count 8 charges Ms. Thompson with transmitting a program information code and command to a computer intending to cause damage.

Count 9 charges Ms. Thompson with access device fraud under 18, United States Code section 1029.

And then Count 10 charges Ms. Thompson with aggravated identity theft under 18, United States Code, section 1028(a).

This means Ms. Thompson is alleged to have knowingly possessed without legal authority the means of identification of another person during and in relation to wire fraud as charged in Count 1, or access device fraud as charged in Count 9.

Ms. Thompson is accused of doing so, knowing that the means of identification belong to a real person.

And these acts are all alleged to have occurred in Seattle, Washington.

Now, Ms. Thompson has entered a plea of not guilty to all of these counts. And she is presumed innocent. She has no obligation to testify. She has an absolute right to remain silent. The burden of proof to prove these charges beyond a reasonable doubt rests on the government.

The evidence you are to consider in deciding what the facts are consists of the sworn testimony of any witnesses and the exhibits that are received into evidence, and any facts upon which the parties agree or stipulate.

The following things are not evidence and you must not consider them as evidence in deciding the facts of the case:

First, the statements and arguments of the attorneys are not evidence. Their opening statement and closing argument are intended to help explain the case to you, but what the lawyers say is not evidence.

Questions and objections of the attorneys are not evidence, and any testimony that I strike or instruct you to disregard is not evidence.

And finally, anything you see or hear when court is not in session is not evidence, even if what you see or hear is said by one of the witnesses or one of the parties.

Evidence may be direct or circumstantial. Direct evidence is direct proof of a fact, such as testimony by a witness, about what that witness personally saw or heard or did.

Circumstantial evidence is indirect evidence that is proof of one or more facts from which you could find another fact.

You are to consider both direct and circumstantial evidence. Either can be used to prove any fact.

The law makes no distinction between the weight to be given to either direct or circumstantial evidence. It is for you to decide how much weight to give to any evidence.

There are rules of evidence that control what can be received into evidence. When a lawyer asks a question or offers an exhibit into evidence and the lawyer on the other side thinks it is not permitted by the rules of evidence, that lawyer may object. If I overrule the objection, the question may be answered or the exhibit received. If I sustain the objection, the question cannot be answered and the exhibit will not be received.

Whenever I sustain an objection to a question, you must ignore that question and not guess what the answer would have been.

Sometimes I may order that the evidence be stricken from the record or that you disregard or ignore the evidence. And that means when you're deciding the case, you must not consider the evidence that I told you to disregard.

In deciding the facts in this case, you may have to decide which testimony to believe and which testimony not to believe. You may believe everything a witness says, part of it, or none of it.

In considering the testimony of any witness, you may take into account the witness's opportunity and ability to see or hear or know the things testified to, the witness's memory, the witness's manner while testifying, the witness's interest in the outcome of the case, if any, the witness's bias or prejudice, if any, whether other evidence contradicted the witness's testimony, the reasonableness of the witness's testimony in light of all the evidence, and any other factors that bear on believability.

You must avoid bias, conscious or unconscious, that's based on a witness's race, color, religious beliefs, national ancestry, sexual orientation, gender identity, gender, or economic circumstances in your determination of credibility.

The weight of the evidence as to a fact does not necessarily depend on the number of witnesses who testify about it. What is important is how believable the witnesses are and how much weight you think their testimony deserves.

I want to say a few words about your conduct as jurors. You must keep an open mind throughout the trial and not decide what the verdict should be until you and your fellow jurors have completed your deliberations at the end of the case.

You must decide the case based only on the evidence received in the case and on my instructions as to the law that applies.

You must not be exposed to any other information about the case or the issues it involves during the course of your jury duty.

Thus, until the end of the case, or unless I tell you otherwise, do not communicate with anyone in any way and do not let anyone else communicate with you in any way about the merits of the case or anything to do with it.

This restriction includes not discussing the case in person, in writing, by phone, tablet, computer, or any other means, email, texting, et cetera, et cetera.

This restriction applies to communicating with your fellow jurors until I give you the case for deliberation, and it applies to communicating with everyone else, family members, employers, et cetera, et cetera. And of course, not at all to the media.

But if you are asked or approached in way about your jury service or anything about this case, you must say that you have been ordered not to discuss the matter.

And if you have such contact, report it to Victoria as soon as you have it.

Because you will receive all the evidence and legal instructions you properly may consider to return a verdict, do not read, watch, or listen to any news or media accounts or commentary about the case or anything to do with the case. Do not do any research, such as consulting dictionaries, the Internet, or any other news or media accounts or commentary. Do not do any research, do not make an investigation or in any other way try to learn about the case on your own. Do not visit or view any place discussed in the case. Do not do any research about the case, the law, or the people involved.

If you happen to read or hear anything about the case, just turn away, report to me what you heard, and we'll just deal with it from there.

These rules protect each party's right to have a case decided only on the evidence that has been presented here in court.

Witnesses here in court take an oath to tell the truth. And the accuracy of their testimony is tested through the trial process.

If you do any outside research or investigation or gain any information through improper communications, your verdict may be influenced by inaccurate, incomplete, or misleading information.

Each of these parties is entitled to a fair trial by an impartial jury. And also, it is required that you decide the case based only on the information presented in court. And you will have denied the parties a fair trial if you go by outside information.

Remember, you've taken an oath to follow the rules. And it is important that you live up to that oath and follow these rules.

A juror who violates these restrictions jeopardizes the fairness of the proceedings, which could result in a mistrial that would require us starting all over again. If any juror is exposed to outside information, please notify us immediately.

At the end of the trial, you will have to make your decision based on what you recall of the evidence. You will not have a written transcript of the trial, so I urge you to pay close attention.

If you wish, you may take notes to help you remember the evidence. And if you do take notes, please keep them to yourselves until you and your fellow jurors go to the jury room to decide the case. Do not let the note-taking distract you from being attentive.

Now, we're going to actually pass out notebooks and pens, which some of you have never used probably, or at least for the last couple of decades. But the notepads will be numbered 1 through 15. You now have new juror numbers based on your seats;

1 through 8 in the back and 9 through 15 in the front.

And whenever you come out to the courtroom, Victoria will have those notebooks on your chair. When you leave, just leave them on the chair and she'll collect them.

No one will read your notes. And whether or not you take notes, you should rely on your own memory of the evidence. Notes are only there to assist your memory and you should not be overly influenced by the notes of either yourself or your fellow jurors.

Okay. The next phase of the trial will now begin.

Ms. Manca, Assistant U.S. Attorney, will make an opening statement, and then Mr. Klein on behalf of Ms. Thompson will make an opening statement.

An opening statement is not evidence, it is simply an outline to help you understand what that party expects the evidence will show. A party is not required to make an opening statement, but both sides will make opening statements here.

The government will then present evidence, and counsel for the defendant will cross-examine the witnesses.

If the defendant chooses to offer evidence, and she's under no obligation to do so, Counsel for the government may cross-examine those witnesses.

After the evidence has been presented, I will instruct you on the law that applies to the case and the attorneys will make closing arguments.

After that, you will go to the jury room to deliberate on your verdict.

A defendant in a criminal case has a constitutional right not to testify. In arriving at your verdict, the law prohibits you from considering in any manner that the defendant did not testify.

Proof beyond a reasonable doubt is proof that leaves you firmly convinced the defendant is guilty. It is not required that the government prove guilt beyond all possible doubt. A reasonable doubt is a doubt based upon reason and common sense and is not based purely on speculation. It may arise from a careful and impartial consideration of all the evidence or from lack of evidence. If, after a careful and impartial consideration of all the evidence, you are not convinced beyond a reasonable doubt that the defendant is guilty, it is your duty to find the defendant not guilty.

On the other hand, if, after careful and impartial consideration of all the evidence, you are convinced beyond a reasonable doubt that the defendant is guilty, it is your duty to find the defendant guilty.

Okay. So now we're going to move to opening statement.

And please give your attention to Assistant United States Attorney, Jessica Manca.

GOVERNMENT'S OPENING STATEMENT

MS. MANCA: May it please the Court, Counsel, members of the jury: I'm a crook. Those are the words the defendant herself used to describe her conduct in this case.

She boasted about having terabytes of Capital One's data. That's not all she said, but that's probably the most egregious.

She bragged about making a six-figure salary for herself mining cryptocurrency with other people's computing power.

And the evidence will prove that what she said in those online chats and so many other online chats was true.

Paige Thompson is a longtime Seattle resident. She is a systems engineer and a software engineer who has over 10 years of experience working for various technology companies in the Seattle area, including Amazon.

In her personal life, she used the online nickname "Erratic."

The defendant is charged with illegally hacking computer networks. She specifically targeted computer networks or companies that were renting computing power from her former employer, Amazon. She scanned millions of Internet protocol or IP addresses looking for a very specific vulnerability.

When she found that vulnerability, she exploited it to steal security credentials. Once she had the security credentials, she used them to access the victims' AWS, Amazon Web Services account, steal data, and mine cryptocurrency with other people's computing power.

That is how she stole over a hundred million people's personal identifying information from Capital One. That is how she stole a million customer records from a company called Survox. And that is how she stole source code from a company called Apperian, and it's how she made over $5,000 a month mining cryptocurrency using servers on other people's AWS accounts.

The evidence will show that she did this primarily to make money, to prove that she was smarter and more skilled than the people that she hacked, and to brag about her exploits online.

This is not a case about a person who opened up Internet Explorer, started surfing around the Internet, and stumbled into a pile of Social Security numbers by accident.

You will hear a lot of evidence in this case about the defendant's methodical multistep hacking process, about the scripts that she refined over months of continuous work, and then ultimately put in a file she titled aws_hacking_shit.

You are going to hear that she used a Linux command line console to issue sophisticated commands that targeted a very specific vulnerability.

And for illegally hacking companies to steal their data and steal their computing power to mine cryptocurrency, Paige Thompson is charged with 10 counts.

Now, much like Judge Lasnik did just a moment ago, I'm not going to instruct you on the full elements of each of these charges, we'd be here probably all morning. What I'm going to do is give you an overview of what these charges are so that you have a sense of what the evidence will be as it comes out. But, remember, the judge is going to instruct you on the law at the end of this case.

So the indictment alleges Count 1, a scheme to defraud, it's called wire fraud, which is using stolen security credentials to download private data and steal computing power to mine cryptocurrency. So the intent to deceive and to cheat is to take the data and to steal computing power.

Count 2, 4, 5, 6 and 7 allege breaking into a computer without authorization and downloading private data.

One of the things the government will prove in this case is that the defendant acted without authorization. Authorization is different from access. If a stranger guesses my password and logs into my email account and starts downloading my emails, right, that person has access to my email account, but not authorization.

Count 8 alleges a crime that is going to be colloquially referred to as cryptojacking, and it involves installing a cryptomining program that deletes logs on victim company computers and racks up bills on their Amazon accounts.

And Counts 9 and 10 allege attempting to possess more than 15 access devices, with intent to commit fraud involving a real person's identification.

This is a computer hacking case, so of course you're going to hear a lot of technical terms and testimony throughout the trial. Some of you have a strong background in technology, some of you don't. For those of you who don't have a background in technology, don't worry, the witnesses are going to take their time to break down these concepts and explain them in basic terms.

Again, I'm not going to go into every term, every concept, every fact you're going to hear in trial, like this is the preview of what's going to happen, and we don't want to be here all morning.

I'm going to give you a bit of a road map. I'm going to take about 30 minutes to explain some of the top five or six terms you're going to hear to give you a high-level overview of the defendant's hacking scheme and then explain how she got caught.

So the first term you're going to need to know is something called cloud computing. This is a bit of a misnomer, right, there is no cloud, I'm sorry to say, that has all of these computing resources.

When companies started using computers, they bought their own equipment, they maintained their own equipment in their own office space, but that can get expensive, the cost of, you know, maintaining the equipment, updating the equipment when it gets old, real estate space for the servers. And so companies like -- little ahead of myself. Companies like Amazon and Microsoft thought to themselves, what if we put, you know, these -- what if we make these massive data centers and we place them throughout the world and we offer companies computing power as a service. And so that's all cloud computing is, it means that I am located physically here and I am renting computing power from a data center somewhere else, and that data center is owned and maintained by someone else.

Amazon has a cloud computing service, they call it Amazon Web Services. And you'll hear that the defendant specifically targeted customers of Amazon Web Services.

The next term to know is metadata, okay. Metadata is information about information, okay. And if that concept is so abstract that it makes your head hurt, you know, like, you're not alone, right. But the good news is that you have probably already interacted with metadata in your own life already, right. This is an example. This is a photograph, right. And what -- the information about the photograph is all metadata, right. Information about, you know, what kind of device took the photograph, where the photograph was taken, how big a file it is, things like that, information about information, that's what we're talking about when we talk about metadata.

So how does this relate to cloud computing? Well, the challenge that cloud computing has to solve is you've got these physical data centers, you know, all over the world, but they're running computing power for companies all over the world. And so how do you keep which virtual machine is going to which company straight. And the way you do that is with something called a hypervisor, that's the graphic in the middle. Hypervisor is kind of a cool name. But what it does is it keeps track of which virtual machines are running in which places. And so it stores kind of information like what AWS account am I associated with. What IP address do I have. What security credentials can access me. All of this is information that if the virtual machines want to know information, they can ask the hypervisor.

So this is metadata, right, information about the servers. An instance is Amazon's names for servers, and this service of providing information.

So, again, instance metadata service this process of asking the hypervisor for information about virtual machines. And all of this is just supposed to be internal inside the cloud environment.

But what you can see is that this information, particularly that bubble on the right, makes this metadata a very juicy target for hackers. This is where Paige Thompson stole the security credentials that she used to later access victims' AWS accounts.

The type of credentials she stole are something called IAM Role credentials. IAM is an acronym for identity access management, right, that is the foundation for security on Amazon

Web Services' cloud platform. And so Amazon Web Services has a user account that you might be more familiar with, with a user name and password.

Role credentials are a little different in that they're permissions to do certain things with services and resources in the cloud environment. So they can be used by people, but more often they're used by machines.

So a company can create something called a billing role, and they can assign it to this application right here. So let's say this is a billing application that needs to generate invoices for -- for customers or for a client, they -- the billing application will go to the database and say, I need your customer information to generate these billing invoices, here's my IAM Role credential, give me access to this customer data. And the database says, sure, billing application, I see your IAM Role, I see your credentials, here's the customer information.

And this is happening in the background of machines, you know, services, applications talking to each other with these credentials over and over and over again, millions of times a day in the background, right?

Next term, proxy. Okay. Proxy is very similar to what you might know in real life. Someone sends someone to the meeting to vote on their behalf, it's referred to as a proxy. That's what a proxy is is an intermediary forwarding on a request. So a source says, you know, hey, I want, you know, this thing, and the proxy sends it to the destination. The destination gets whatever thing was requested, forwards it back to the proxy, and then back to the source. It's just an intermediary forwarding things on.

And where that comes up is in something called a reverse proxy. So when you open up Internet Explorer, let's say you want to check your driver's license, so you go to the DOL website, you will likely interact with a reverse proxy. The reverse proxy will send your request to the internal server that actually has that information, serve it back up to the reverse proxy, and then the reverse proxy serves it back up to you on your computer screen in your web browser.

Another term, web application firewall -- oh, getting back to this point, why would a company want a reverse proxy, as opposed to just having their external device connect with their internal server directly, right. The reason is that it provides an extra layer of protection from the Internet. So by having that intermediary, that intermediary step just gives the internal server an extra layer so it's not getting hit by the Internet traffic directly, that's why you do it.

Another layer of protection that companies can add is a web application firewall. The web application firewall sits on the web server, right, so related to the drawing I just showed you, and it acts like a filter for the web server, letting traffic through, you know, filtering other traffic out.

The best way to think about a web application firewall is like a traffic cop, right, sitting on the web server. So, like, you, through; you, through; you, stop, right. That's a web application firewall, it's a traffic cop.

And the last concept we're going to talk about for technology is something called a server-side request forgery, or SSRF, which is a common term in technology.

Normally, when someone makes an external request that they aren't authorized to make, the external user will say to the web server, I want to do this thing, like, say, for example, instead of looking up information about my driver's license, I want to look up something about my neighbor's driver's license. I send that request to the reverse proxy, the reverse proxy sends it to the internal server, and the internal server, she doesn't have authorization to look up her neighbor's driver's license, and sends back a request denied message or something like that.

A server-side request forgery looks a little different in a couple of ways.

Number one, the request looks like it's coming from that internal component. So the internal server that's receiving that information, instead of saying, oh, no, an external user doesn't get access to this information, says, oh, sure, good buddy, we're on the same network, of course you can have that, right. So that's one thing that's different.

The other thing is that the request is going somewhere else. So instead of going to the internal server to ask for information about drivers' licenses, it's going to say like a database of information about DMV employees. So those two things, the request looks like it's coming from an internal source; and number two, it's going somewhere different than the way the web traffic was supposed to go.

And you'll hear testimony from an FBI computer scientist about how the scripts that he reviewed on Paige Thompson's computer show that her attack relates to a server-side request forgery.

So how did the defendant hack these companies? Well, the first thing she did was hide her identity online. You'll hear about her use of a virtual private network or VPN service called iPredator and another anonymizing server called The Onion Router or TOR.

These services have a lot of uses, you know, many of them legal, but one of the uses for these two services is to hide your IP address when you're committing crimes so that no one can trace your Internet activity back to your home internet.

And in an online chat, the defendant, using the screen name Erratic, described to a friend about the information she had stolen from these companies she was hacking. And the friend said, sketchy stuff, don't go to jail, please. And her response was, I'm like iPredator, TOR, S3 on all of this, meaning she's anonymizing her traffic, they won't know it's her. I want to get it off my server, that's why I'm archiving all of it. LOL. It's all encrypted. I just don't want it around, though. I've got to find somewhere to store it.

You'll hear that she stored company data in a folder called aws_dumps. She stored her scripts in a folder called aws_hacking_shit. She developed a computer program that scanned tens of millions of Amazon Web Services IP addresses looking for a very specific network vulnerability. This is one of her Google searches.

In network computing, all of the web-facing components of a system and all of the internal components are supposed to work together harmoniously, but the process of putting those together is complicated. And so sometimes the web-facing external components and the internal components don't work together the way they're supposed to because of mistakes in code. Those mistakes in code are referred to in text speak as a misconfiguration. The defendant was looking for a very specific misconfiguration in the way companies' web-facing external components interacted with the internal components, and that misconfiguration allowed her to access that hypervisor with those juicy security credentials.

When she found the specific misconfiguration she was looking for, she exploited it to steal security credentials.

This is one of her hacking scripts. You'll see a larger version of it when the witness testifies or the government's expert witness testifies, but she gave this script the label "#getsecuritycredentials." And that's exactly what it does. It grabs the security credentials, and then this script at the very bottom at the end, awssession.sh, plugs in the security credentials with this, the secret access key, the session token, and the access key for those security credentials, the IAM Role that I told you about earlier.

And once she had these security credentials, she could use those credentials to actually log in to the customer's AWS account. It's just like finding a password and using it to log in to someone's email.

The defendant described what she was doing in her own words in this Tweet from June of 2019. She said, And then I hack into their EC2 instances, which are virtual machines, assume-role their IAM instance profiles, that's taking over that role credential, take over their account, again in her own words, mirror their S3 buckets, which means download their data, and then she's talking about the process of storing the data on her own server.

As the defendant said, yeah, AWS is great, except when someone steals your IAM instance profile that has full access to the account. Smiley face.

Once she was logged in, she had the power to do whatever the credentials had the power to do. For some companies, it was access to their data; for other companies, it was adding computing resources to the company's account that she could use to mine cryptocurrency. For some companies, it was both the power to download data and the power to add those resources.

I mentioned the folder where she stored the company data called aws_dumps. The defendant downloaded Capital One's data on March 22nd, 2019. In this trial, you're going to hear about a mysterious note that an unknown person passed to an Amazon employee at an Amazon conference in Seattle sometime in March -- I'm sorry, May of 2019, two months after the Capital One hack. The note said there was an open SOCKS proxy at one of Capital One's IP addresses that exposed internal security credentials. Amazon forwarded the note to Capital One. But Paige Thompson did not use a SOCKS proxy to commit this attack and access Capital One servers, even though that uses the word proxy. The technical expert will explain why that's different. It's a different network layer, a different communication language.

Capital One did not find the vulnerability when they received that note because they were looking in the wrong place. It was only two months later in July of 2019 after the events I'm about to talk about that Capital One thought maybe that note was describing a vulnerability like the one that Paige Thompson exploited. It was a real, if I'd only known then what I know now, kind of moment.

But regardless, even if Capital One had figured out in May 2019 what that note meant, it wouldn't have stopped the defendant from downloading their data because she'd already done that two months earlier, the data that the defendant downloaded into this aws_dumps folder. And it wasn't easy to read or access.

Once she realized that she had caught millions of people's names, address, emails, phone numbers, and security numbers, Social Security numbers, in the illegal net that she was casting, she looked for ways to make money off the data. She searched through it. She organized it. She looked for better ways to organize it. She put together a list of personal identifying information for people who lived in Seattle.

She searched for carding forums on the dark web, places where people sell information that can be used to commit credit card fraud.

In an online chat, she talked about "thinking about carding a lot lately." She talked about algorithms that people use to prevent credit card fraud, an embosser, needing to go shopping.

At the same time she was thinking about carding a lot, she was looking up server rentals in Russia where it would be much more difficult for law enforcement to get to this data.

And this is a chat from a few weeks later where she's still looking for a place to upload all of these people's personal identifying information.

The other thing she did when she stole security credentials was create new servers on people's accounts. The reason she wanted to create new servers is that she was doing something called cryptocurrency mining or cryptojacking. I'm sorry, so those two concepts are different. But she was cryptomining using other people's computing resources, which is referred to as cryptojacking.

You've probably heard about cryptocurrency at some point, maybe even seen like a Super Bowl commercial about it. The most well-known cryptocurrency is Bitcoin. There is a way to generate cryptocurrency called cryptocurrency mining. Cryptocurrency mining is completely legal, but it requires a lot of computing power. So sometimes people do the cost-benefit analysis and they think, you know, I'm not going to make as much cryptocurrency mining as I'm going to spend on computer hardware and electricity, so it really doesn't pencil out. But if someone steals computing resources and electricity from someone else, then the rewards that they make from cryptocurrency mining are a hundred percent profit. That's why it's called cryptojacking. Cryptocurrency mining is the crypto, jacking is stealing.

It's a great way to make money out of thin air, but it's illegal.

This is a text message from the defendant's cell phone. She said, "I have about $5,000 a month coming in now, but it's all in Ethereum," which is a type of cryptocurrency, "and I have to find a safe way to convert," meaning convert to fiat currency or U.S. dollars.

"Because I'm hacking AWS accounts to get it using EC2 GPU miners." EC2 is a reference to those virtual computers. GPU is graphic processing unit, meaning high-compute-power virtual machines that can run these cryptocurrency mining programs.

This is code from the defendant's computer. The highlighted portion is, again, that script that takes those security credentials. CICD instance is the company's IAM Role credential. "awssession.sh" plugs in that secret access key and token, giving her access to their account.

Once she's inside their account, she runs all those instances, meaning creates all those servers on their account. And the reason this company, it's called Survox, found out about this, about these servers on their account, is that they got this bill for over $53,000 in the mail for one month. They normally run a bill of about $8,000.

So they called up Amazon and said, what is this bill. And Amazon says, well, you have all these high-computing servers running, you know, in Dublin, Dublin, Ireland. And they said, we don't have any servers in Dublin, Ireland. And Amazon eventually refunded the money and they, Amazon, took the loss.

This is another chat from the defendant's computer, I've gone to my counselor, told her I was hacking and stealing CPU time to mine crypto and buying new things for myself and wearing new designer clothes, et cetera.

And the last part I'll talk about with respect to cryptocurrency mining or cryptojacking is this script, "minersetup_eth.sh." This was in the aws_hacking_shit folder. The script is much longer than this, and the testimony will describe what this script does. But this piece of script right here is how -- one of the ways that the defendant covered her tracks when she was planting this cryptocurrency mining program. It deletes the logs or the records of her activity on the victims' servers. But it doesn't just delete the log of her activity, it deletes all the logs, so the logs that the company would need to have a record of what was happening on their servers would no longer exist.

She talks about another way that she covered her tracks with the cryptojacking in this online chat. She said, "I changed the script to move everything and all the work on the ram disk which effectively leaves the customer unable to do any kind of forensic recovery."

She also talked about the script disabling journaling on the file system live, or that that was one of the things she wanted to do.

And then she used this emoji, xD, because it's very funny to remove customers' ability to do any kind of forensic recovery on their electronic devices.

So how did she get caught? Well, one day in June 2019, she started boasting about her hacking activities to a random person on the internet. Specifically, the defendant sent a series of private Twitter messages, or direct messages, DMs, to a woman named Kat Valentine.

At the time, Ms. Valentine had been posting online about a line of shoes with hacker themes that she was going to design and thinking about selling.

Ms. Valentine has a technology background, she works in technology compliance, and considered herself part of the information security community.

Kat Valentine did not know the defendant. They had never even chatted online before. And the defendant messaged her with this essentially out of the blue. "Jacked" and then there's a link to something called a GitHub Gist, all available S3 bucket, certs.

S3, Ms. Valentine knew, is terminology that Amazon uses for its storage mechanism. So an S3 bucket is just somewhere that companies can store information in the cloud.

There was a link to a GitHub Gist, which is essentially a place that people can post code to share.

Three terabytes of S3 buckets.

"Are we there yet?" Meaning have you figured out what I've done.

Kat Valentine did not know the -- and these messages continued for several days.

I basically strapped myself with a bomb vest, dropping

Capitol One's dox and admitting it. I want to distribute these buckets I think. They're SSNs, Social Security numbers, with full name and DOB, meaning date of birth.

She threatened to give all of this to a desperate "Chinese dude who scams people for research chems on Reddit and drug forums." And said, "I don't care anymore." She said she deserved to be exposed and it was time to go to jail.

Ms. Valentine had no context for any of this. Like I said, she didn't know the defendant. And these messages are a lot to absorb.

So a couple weeks later -- well, first, what she did is she blocked the defendant on Twitter. But a couple weeks later, a conversation with a friend jogged her memory about these Tweets and she decided to click on that GitHub link, and what she found again was a lot to absorb.

This is what the link transferred her to, the GitHub Gist. It's secret, meaning only someone with the link could access this page. But the defendant had sent her the link, so she was able to access it.

The post referenced security credentials. But what really captured Kat Valentine's attention was this, row after row after row of file names, over 40 pages of them, like card-prod-west. From her experience in technology compliance, she knew that meant credit card information.

She scrolled all the way to the last page and she saw this, four letters, s-y-n-c, sync. That meant the defendant had not only looked at those bucket names, all those folders with credit card information, she had downloaded them.

And all of a sudden the defendant's claims became very real, threatening to distribute Social Security numbers, dates of birth, and she knew she had to report the breach to Capital One. She Googled responsible disclosure, Capital One.

Now, like most companies, Capital One has a responsible disclosure program. Responsible disclosure is a way that tech people who find network security vulnerabilities can report those vulnerabilities to the affected company and work with the company to fix the vulnerability. Some companies even pay people who help them find and fix vulnerabilities, something referred to as a bug bounty, which is a payment for helping companies find and fix vulnerabilities.

But there are strict rules around security research and responsible disclosure in technology. A person can't cross certain lines, like downloading data, or installing programs, or deleting files. It's a bit like being a doctor, you know, do no harm, don't kill the patient.

So on July 17th, 2019, Kat Valentine Googled responsible disclosure, Capital One, and found a web page about Capital One's responsible disclosure program. They accept responsible disclosure submissions through the creatively named email address, responsibledisclosure@capitalone.com.

Ms. Valentine sent that gist link, that code link, to that email address.

Someone at Capital One reviewed her email and the link and almost immediately realized that they had a very serious problem on their hands.

Suffice it to say that a lot of people at Capital One did not sleep very well for the next few days.

Capital One figured out a couple of things very quickly. Number one, they realized how they had been hacked based on the information that Ms. Valentine had sent; and number two, they realized that Paige Thompson was the hacker. It frankly wasn't hard to figure out that Paige Thompson was the hacker. Her name was on that GitHub link, as you've just seen. And when Capital One and later the FBI surfed around some linked web pages and social media profiles, they found a resume with her address in Seattle, said she used to work at Amazon, and she's familiar with Amazon Web Services' cloud computing technologies, like S3, EC2, and IAM.

Capital One offered to pay Kat Valentine for the information she provided for the breach, but she actually turned down the money.

Capital One also contacted the FBI within days of realizing they had been breached. And for the FBI, it was a race against time to serve a search warrant on the defendant's house to recover all of those names, birthdays, dates of birth, addresses, phone numbers, email addresses, Social Security numbers, before the defendant uploaded them somewhere or distributed them to a scammer like she had threatened to do in those Twitter messages.

On July 29th, 2019, the FBI served a search warrant on the defendant's house and seized this very large custom-built desktop computer.

They were able to access that folder -- or that computer and found the aws_dumps folder where the defendant stored all the data she had stolen, including Capital One's and other millions of people's personal information.

The FBI got to all of that data before the defendant ever distributed it or uploaded it anywhere.

The defendant talked to the FBI while they were at her house. The case agent, Joel Martini, will tell you what she said to them. She lied to them. Pay attention to what she chose to lie about, because the things she chose to lie about were evidence of how far she had crossed the line in breaking the law.

For example, she said she did not use iPredator or TOR. She said she did not remember if she downloaded the data. She said she did not try to look at the content of the data. She said she probably deleted the data. She said she would not have put the data on her server.

She didn't say anything about trying to work with these companies to fix their vulnerabilities or making any kind of responsible disclosure. She said she had only told one person about the hack, which turned out not to be true. But if there was a time to talk about responsible disclosure, that was it.

You are going to see a lot of evidence in this case that the -- that is completely inconsistent with the defendant acting in good faith to help protect and improve network security.

Some of the evidence you will see, for example, is that she hacked companies once and then came back to hack them again. You will see again and again and again that she had numerous opportunities to stop, but didn't stop. She was making money off of these companies. And the more she took from them, the more she could brag about it online. She didn't want to help them.

For example, she shared her hacking script with a friend in an online chat and then wrote, Yeah, if you want to use it to learn how to do some stuff with AWS, go for it, it's not my stuff. LOL.

In March 2019, while describing her hacking scheme to a friend, Paige Thompson wrote this text message, They'll have to prove it's me. And second, it's the user's fault for letting it happen.

Several months later, the defendant admitted it was her and that's why she was caught.

So what you can expect is that this trial is going to focus a lot on that second part, that it's the user's fault for letting it happen. And this will be a little bit like blaming the security guard for failing to stop the bank robbery.

Remember, at the beginning of this statement, I talked about the difference between access and authorization. The defense will try to convince you that access and authorization are the same, that a mistake that provides access is the same as authorization. And you will definitely hear about technological mistakes that companies made, particularly Capital One.

Capital One was fined $80 million by its regulatory agency for failing to adequately prevent, detect, and mitigate Paige Thompson's attack. And when you hear the evidence in the case, you may even think that Capital One deserved to get fined. That perspective won't be inconsistent with anything the government needs to prove at trial, because this trial is about addressing Paige Thompson's role in the breach.

Anything that Capital One did wrong will not make Paige Thompson right in what she did. Failing to prevent, detect, and mitigate an attack is very different from authorizing it to happen.

Paige Thompson was not authorized to grab security credentials from internal metadata and use those credentials on a company attack -- a company account as if they were her own. And that is particularly true because she actually knew she was in a place she wasn't supposed to be, doing something she wasn't supposed to do.

In her own words, as you've just seen, she said she was stealing credentials, stealing data, and stealing computing power.

What she did was illegal, she knew it was illegal, she just did not care.

And at the end of this case, after you've heard all the evidence, my colleague, Andrew Friedman, will stand here and ask you to return the only just verdict in this case, which is guilty to all counts.

Thank you for your attention.

THE COURT: Thank you very much, Ms. Manca.

Would you now please give your attention to Brian Klein, who will make the opening statement on behalf of the defendant, Paige Thompson.

MR. KLEIN: Your Honor, can we have a quick sidebar for one minute?

THE COURT: Oh, I don't do sidebars. Sorry.

MR. KLEIN: Okay.

THE COURT: Those of you who remember the O.J. Simpson trial, do you remember there was like one sidebar after another? And I was already a judge, and I was like, never again will I do a sidebar.

But it's almost impossible to do it now with masks, protection, court reporter has to come over here, you know, we have to talk, et cetera, et cetera, so let's just do it, okay?

Yeah. My wife asked me about, how are you going to do sidebars? I said, I don't do sidebars. She said, what do you mean you don't do sidebars?

MR. KLEIN: Well, then I feel like I am in good company.

THE COURT: Yes, you are in good company. She agrees with you, but I'm not doing it.

DEFENDANT'S OPENING STATEMENT

MR. KLEIN: Good morning. My name is Brian Klein. Let me introduce you to the team that's helping defend Paige.

That's Mo Hamoudi, my co-counsel, that's Stacey Brownstein, who is an investigator with the Federal Public Defender's Office.

Sitting along this row are other attorneys, Melissa Meister, Emily Stierwalt, Nancy Tenney.

Together we represent Paige Thompson.

I work at a law firm. We're handling this case pro bono.

Mo, Stacey, Nancy work for the Federal Public Defender's Office.

I want to also introduce you to Paige.

Paige, can you stand up for a second?

THE DEFENDANT: Good morning.

MR. KLEIN: That's Paige Thompson. Thank you.

We all just heard a rather lengthy and complex, at least technology-wise, opening by the government. It's designed to make this case sound like it's over before it starts. It's not.

As Judge Lasnik told you, what we say, what Ms. Manca says what I say, that's not evidence. What we're laying out is a preview of what you're going to hear in this case.

And turning to that, here are some things that we believe the evidence will show:

There are very good reasons Paige Thompson is contesting these charges that the government has brought against her. There are very good reasons that she and we proclaim her innocence. And there are very good reasons after hearing all of the evidence, including the evidence you hear when government witnesses are cross-examined by us, you will find her not guilty.

Let me say a few things up front. Things that Paige doesn't dispute, things that the prosecutor said that make it like she might. Paige doesn't dispute piecing together that short automated scanning program and its various iterations. She doesn't dispute that that program searched the Internet for servers of Amazon customers that were publicly accessible and would grant credentials to anyone who requested them. From there, she doesn't dispute that she would research further and sometimes request those credentials, again, that anyone could get. So you need to pay very close attention to the evidence in this case.

There's a lot more that you're going to hear about than what you just heard from the prosecutor. And what Paige said, those statements, admittedly some of them are ugly, some of them sound incriminating, but that doesn't change other critical facts, and it doesn't change how the law applies to them.

So you need to pay very close attention to the judge's instructions at the end of this case. I know you paid close attention to what he told you this morning. At the end of this case, he's going to reinstruct you, and it's critical that you listen to the judge, because there's a disagreement here about how that's going play out.

We want you to dig into the facts here. We want you to look closer. Take your time, don't accept surface-level explanations by the government or their witnesses. There's a lot of technical stuff in this case. It's going to take time to absorb. It's taken us time to absorb. It's taken them time to absorb. But it's really important that you take that time. And when you spend that time, at the end of this case, what you're going to see here is the evidence will show that the government is trying to criminalize accessing computing networks that are publicly accessible.

Now, let me turn back now to Paige for a moment.

Paige is a lot of things. She is smart. She has strong opinions. She loves technology. She is curious and likes to do deep dives into things. She happens to be transgender and has struggled to find acceptance, like many transgender people. She's often been lonely and isolated and depressed. And like many people in those places, she's found refuge online, because the outside world has rejected her. She can be a big talker online and says many things, many things you saw the prosecutor put up. She can be provocative. She says things to get attention. She says things to get a reaction. She says things because she's under a lot of pressure and stress.

She's also erratic. That's a fitting title that she chose. You may not get Paige, and we're not asking you to. You may not get what makes her tick, and you may not like things she says. I think we can all agree on that, but, again, you need to look closely when you're asked to by the judge at the government's evidence and see if it matches up to the law at the end of this case.

Let me turn back to Paige for a second. I want to give you some more details about her. Paige hails from Arkansas from a broken family. Her dad was never around. Her mom struggled to find well-paying work. She eventually succumbed to drug and alcohol addiction.

You won't see her family here. You may see a small group of supportive friends. But the evidence will also show that Paige moved to the Puget Sound in high school, that she struggled and dropped out of community college, but she was very good at technology. And she had a lot of technology jobs. You saw the prosecutor put up her resume.

Her last job happened to be at Amazon, but she didn't work on the things at issue here. And you're going to hear no evidence and no claims that she used any of the things she learned at Amazon or had any inside secret knowledge about how things worked to undertake the things the government is accusing her of.

Who else will you meet at this trial? There's going to be a lot of witnesses in the next week or two. For one, you're going to meet representatives of some of the most powerful companies in the world, Amazon and Capital One.

The evidence will show that they have powerful financial motives to pin the blame on Paige.

You're going to learn that Capital One, following this incident, came under investigation by their bank regulator and ultimately paid an $80 million fine.

We want you to look closer at the power dynamics at play here, look closer at the evidence.

You're also going to hear from law enforcement agencies. You heard Judge Lasnik instruct you at the beginning how you're supposed to treat the testimony of witnesses. Every witness is treated the same. There's no extra credibility points for law enforcement testimony, none.

Let's turn back to Paige and talk about what happened in 2019. Let's talk about what the government didn't tell you is going to come into evidence. Let's talk about what the evidence will show.

But before I do that, I want to talk for a moment about this online world to give you some context. That may not be the world you spend a lot of time in. Not everyone is online all the time, not everyone is Tweeting, not everyone is posting on Nextdoor, but that's the world Paige inhabited.

And I think we can all know, the evidence will show, people put up a lot of half-baked ideas, say a lot of outrageous things, to get attention. They stream their lives on Instagram, they post wacky things on Nextdoor. So when you see those messages, and you saw some of them, you need to place them in context. You need to look closer. You need to remember how they were said, when they were said, and why.

And the other thing you need to keep in mind is the thing the judge instructed you on at the beginning, the presumption of innocence. So when you look at those messages, when you look at the other evidence, that's the lens you're looking at them through. You're presuming innocence. That's the lens you're going to look at all the evidence in this case through.

So now let's get back to 2019, the time period this was all happening. Paige was unemployed. She lived in a house in south Seattle. She had a lot of roommates. She was online.

She had done a deep dive and she'd pieced together this scanning program that you heard about. There were iterations, but I'm going to call it one program for the simplicity of here. This is a general-purpose tool. And what it did is it scanned the Internet for Amazon servers, customer servers, that were publicly accessible. That's what it did at its core. And they had set their web application firewall, which I know is a big term, WAF, you may have heard that a lot here. But that had been something that made those servers publicly accessible.

So let's talk about that for a moment. Paige could have done this process manually, just so you know. She could have manually searched every server, but she created a program. That's normal. That's what people do in the computer world, they create programs to automate things.

You're also going to learn Paige used common software tools. Prosecutor talked about Linux, that's a common software tool. So she did something everyone does, and she used common software tools to do it.

You'll also learn, which the prosecutor didn't mention, all those IP addresses are publicly available. There's no secret list of them. They're out there. So all 3.7 billion of them, or whatever the number is, using common software tools to create a program to look for IP addresses that are publicly available.

Now, what was the way that those web application firewalls were set up? Let's look closer. That scanning program she created let her know if they were set up in a way such that the data was publicly accessible and would grant permission to anyone to access it. From there, she would research further. She would sometimes ask for those credentials that, again, anybody who found them could ask for.

And you'll learn that that wasn't Amazon that set them up that way, it was the customers, okay. So there was no error in Amazon's code, there was no bug on Amazon's side of the ledger. What you'll learn is it was on the customer's side. They were configured in a certain way.

Now, the word "misconfiguration" is a misnomer. You'll learn from a witness that some people might have wanted to configure their servers that way. They might have chose to set them -- things up that way.

And one thing to keep in mind is Paige had no input or control how they set them up. She created the scanning program to look for publicly available servers. And when she found them, she sometimes went in and requested credentials.

Now, let's talk about a few other things. I want to talk about something else the prosecutor didn't mention that I want you to look closer at. You'll learn that Paige had no idea -- when she found this publicly available server, right, she would have no idea what data was in there. In fact, she wouldn't know what was in there. And this is what the evidence will show. She might have known who it was, but the actual specific data, wouldn't know until she had copied it and put it on her computer.

You'll also learn that those Amazon customers' servers didn't technologically care who she was, they responded to the commands of anybody.

So I want to repeat that, not only were the servers publicly accessible, but anyone could ask them to do the things she asked them to do.

Now, this is something else I want to talk about. Paige was under no legal duty to report what she had discovered. There was no law required when she found these servers, copied the data, to tell anybody; no law. And you'll learn Paige didn't report it to law enforcement.

But what does the evidence show happened after Paige started to undertake this? She freaked out. It shows she let a lot of people know about this in a lot of different ways. And a closer look shows you that she never monetized any of this data. So from March 'til her arrest five months later, she never monetized it and she never shared any of it. She never made a cent and never shared it.

It also shows that about a month after this happened, the prosecutor alluded to it, we're going to talk about a lot more in this case, Amazon received a handwritten note. A distinguished engineer at Amazon in the hotel down the street here received a note that had the IP address of Capital One's server. Amazon passed that note on to Capital One.

They investigated it. They didn't realize what they had until later, but you'll see evidence about that.

The evidence will show that Capital One failed to address this issue. And you heard that the government's going to call a witness, Ms. Valentine, who Paige interacted with on Twitter. Paige disclosed to Ms. Valentine what happened here.

Overall, the evidence is going to show, without Paige, none of this would have come out.

Now, I want to talk for a second about TOR and VPNs, okay? Something the government talked about, but I want to talk about things they didn't talk about.

Let me start with TOR. TOR was founded and developed by the U.S. Navy, a research lab. The main group that supports TOR is a non-profit in Seattle. TOR is used -- is funded by the State Department. TOR is used by companies and people all around the world. Using TOR is legal.

VPNs, same idea, every day in every way, people are using VPNs. The prosecutor's office, the Court, my law firm, Federal Public Defenders, people use VPNs all the time.

How does that relate to this case. And one thing I want to explain, you didn't need to use TOR or VPN to do the things she did. The fact that she might have used them is irrelevant. She could still access all that data without using them, I want to make that very clear. To get to that data, she didn't need to use TOR or VPN, it was still there. She needed to mask who she was to get there.

Let me talk briefly about cryptomining. The prosecutor talked about cryptojacking. I just want to make very clear, because the word "jacking" can be used for things like hijacking or carjacking, there's no evidence of violence. No one claims there's any violence here. I just want to make that very clear to you.

And as the prosecutor acknowledged, cryptomining is legal. Ether [sic] is legal. It's the second most popular cryptocurrency. We will talk more about that during the trial, I want you to pay very close attention to the testimony that comes out in trial about that.

Now let's talk about the charges. And let me tell you why paying close attention is important. I know you know it is. My precision is important, because the prosecutor got up and said there are 10 counts, there's nine. We need to be precise here, we need to pay attention. Paige is only charged with nine counts, and those nine counts, the first one is wire fraud, the next six are Computer Fraud and Abuse Act, and the last two are access device fraud and aggravated identity theft.

And all those charges, including the identity theft, flow from things that we talked about so far, things that, frankly, Paige doesn't dispute.

She created together -- cobbled together this very short scanning program. She went and asked for credentials that anyone could ask for, and then went from there.

And at the end of this trial, Judge Lasnik is going to instruct you on the law. And again, I know you will pay very close attention to that. That's critical here.

So having set the stage, let me just go back and give a little recap before we launch into the witness testimony.

Paige doesn't dispute creating that program, iterations of it. She doesn't dispute accessing publicly accessible data. She doesn't dispute requesting credentials that anyone could ask for. So when you look at that evidence, what you'll see here is the government is trying to criminalize accessing publicly accessible information. That's what Paige did. It's exactly what she did.

All the servers were configured by those customers in a certain way that permitted what happened here to happen.

And let me say this again, nothing she said, no matter how ugly, how upsetting, or even, frankly, how incriminating it appears, changes critical facts, changes the law, changes how you're supposed to look at everything.

Again, you'll see no evidence she profited from anything or that she shared anything. And by that, I mean profited from the data she copied.

So last few points. What we want from the defense is for you to look closer, pay attention, to listen to what's asked, to listen to the cross-examination, to really pay attention to what these witnesses tell you; to get the whole story here, not just the story the government told you in the opening, but the whole story here, because that story is different than the one you heard in the opening from the government.

And we're also going to ask you to put your personal feelings aside about some of those statements that may be offensive to you. That's not what you're here for. You're here to look at the evidence, which I know you will do. You're here to look at it fairly, you're here to look at it with the presumption of innocence. And at the end of the day, Judge Lasnik is going to instruct you, and we believe you will find her not guilty.

Thank you.

THE COURT: Thanks, Mr. Klein.

Okay. We have a situation with the jurors where they're not just going to go back here to the jury room, so I need everyone in the audience to stay seated and not get up, please, until the jury has been allowed to be taken out by the courtroom deputy to downstairs.

So, Victoria, why don't you take the jury down to Judge Pechman's room.

And please stay seated in the audience until the jury has gotten down there.

Will you let us know when you get there?

THE CLERK: (Nodded affirmatively.)

THE COURT: Okay. How will you do that? Send me an email.

THE CLERK: I can do that.

THE COURT: Okay. Great.

All right. Please go with Victoria down to Judge Pechman's room.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: You never have to stand for the jury, you just have to stand for me.

Judge Coleman in King County Superior Court once said that to me when I was a baby prosecutor: The jury just decides the facts, the facts are not that important, but the judge represents the law, so you got to stand for the law.

Did you want to say anything, Mr. Klein? I -- you know, in that aborted sidebar? You don't have to, but...

MR. KLEIN: Your Honor, just that I thought the government offered some legal instruction to the jury there at the end of their close [sic], and I was thinking maybe it would be important that --

THE COURT: Yeah, it wasn't.

MR. KLEIN: -- none of us are offering legal instruction to them.

THE COURT: Well, you offered legal instruction, too, to find her not guilty, that's fine. It's okay.

MR. KLEIN: Yes. And I will continue to offer that instruction.

THE COURT: It's perfectly okay.

All right. So, again, please wait just a couple of minutes 'til I know that they're on the elevator.

Maybe my CSO can tell me.

Yes, sir.

MR. KLEIN: One other thing, Your Honor. Sorry.

THE COURT: Let me just ask, Mr. Court Security Officer, were the jurors already on the elevator downstairs, could you tell?

SECURITY OFFICER: There were a few, yes.

THE COURT: Were they still waiting for the elevator or --

SECURITY OFFICER: No.

THE COURT: No. Okay. They're gone. Thank you.

Yeah.

MR. KLEIN: Your Honor, I just wanted Your Honor to know that we reached agreement with the government. And I just -- Professor Halderman is here, just so you -- right there, Your Honor, and will be sitting here throughout the trial, not -- even though he may be a witness and not excluded.

THE COURT: Yeah. That's fine. Whatever you guys agree on is perfectly okay.

Okay. So we'll take our break now, and we'll start up again at 11:00; okay?

All right.

(Court in recess 10:43 a.m. to 11:10 a.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Okay, you have in front of you now those high-tech, note-taking devices with the strange object that puts ink out. Yeah, you get where I'm going on this.

It took us a long time in the legal system to allow jurors to take notes. Even when I used to try cases, there were no notebooks or anything like that; you just had to remember things. So we move slowly, but we move -- slowly, actually, no doubt about it.

So anyway, you don't have to take notes if you don't want to, but if you want to, go ahead. I've already described to you that you should use your memories about what the witness testimony is and not be overly influenced by your notes or the notes of others, and we'll just leave the notepads on the chairs.

The government, please call your first witness.

MR. FRIEDMAN: Your Honor, the government calls Steve Schuster.

THE COURT: Okay. Mr. Schuster -- is -- you can have your witness in the courtroom when we're coming from a break or anything.

MR. FRIEDMAN: Okay.

THE COURT: Mr. Schuster, please raise your right hand to be sworn.

STEVE SCHUSTER,
having been first duly sworn, testified as follows:

THE CLERK: Please state your name for the record, and spell your last name for the court reporter.

THE WITNESS: My name is Steve Schuster; last name is S-c-h-u-s-t-e-r.

THE COURT: All right. Thank you, Mr. Schuster. Go ahead, Mr. Friedman.

MR. FRIEDMAN: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good morning, Mr. Schuster.

A. Good morning.

Q. Where did you go to college?

A. I went to University of Maryland for my bachelor's degree and Cornell University for my master's.

Q. What did you study your major in when you got your bachelor's degree?

A. My bachelor's degree is in computer science.

Q. Okay. And at some point after college, did you start working in computer network security?

A. I did.

Q. When did you do that?

A. About 1992.

Q. Where were you?

A. I was with Bell Labs in the Washington, D.C. area.

Q. And did you continue working in computer network security at Bell Labs for a number of years?

A. I did, through various roles; first as a software developer, and then as a consultant and an advisor.

Q. How long did you stay at Bell Labs?

A. About 11 or 12 years.

Q. Roughly, when did you leave?

A. 2003.

Q. Where did you go after working at Bell?

A. I went to Cornell University.

Q. And what was your job at Cornell?

A. Chief information security officer.

Q. Can you tell us, what is a chief information security officer?

A. So the primary role is to understand where the data are in our networks, in our computers, and ensuring that the network itself is secure and the computers that we use are secure, to make sure that we have a secure computing environment, to protect the data and the users of those computers.

Q. And I assume if you're the chief information security officer, there are people working below you?

A. There are.

Q. How long did you continue working at Cornell University?

A. I was there just under 11 years.

Q. And when did you leave?

A. November of 2013.

Q. Did you switch to another job after you left Cornell?

A. I did. I joined Amazon Web Services.

Q. What job did you take at Amazon Web Services?

A. I took the director of security incident response -- security incident and response and engineering.

Q. Okay. Now, Amazon Web Services is part of another company; is that correct?

A. It's part of Amazon, correct.

Q. And what part of Amazon -- when we think of Amazon, what do most people think of?

A. They think of the retail side of the business, ordering books and other products.

Q. Is that what Amazon Web Services does?

A. We do not.

Q. What does Amazon Web Services do?

A. Amazon offers a set of services and infrastructure called "the cloud" that companies can use to host their services or products.

Q. Okay. Computer services, basically?

A. Typically, yes.

Q. Okay. And you said -- I think you said you were the incident response leader; is that correct?

A. Yes.

Q. As incident response leader, what are your responsibilities?

A. So any potential security issue that we become aware of comes to my team. We do initial triage to understand the issue, understand the severity of that issue, making sure that, if we need to, fix it in necessary time, and then respond and correct the issue.

Q. Okay. Is it fair to say Amazon Web Services -- we call that "AWS"?

A. AWS.

Q. Does AWS have computers and servers --

A. We do --

Q. -- around the world?

A. Yes.

Q. If someone breaks into a facility where you have computers, is that something you're responsible for dealing with?

A. It is. I have a team that monitors the physical security of our data centers, and then would dispatch and ensure that it gets corrected.

Q. What about if someone uses technology and hacks into computers; is that something you might be responsible for?

A. That would be another team of mine, yes.

Q. So all aspects of security?

A. Most aspects of security.

Q. Fair enough.

Roughly, how many people do you have that work for you in this role?

A. It was, roughly, about 600.

Q. Mr. Schuster, I'm going to ask you to explain some technology concepts that might seem basic to you.

A. Yes.

Q. Are you aware of the Internet?

A. I am.

Q. Okay. Do you have a general idea what that is?

A. I do.

Q. Have you looked at Exhibit 101 prior to testifying?

A. I did.

Q. And if we could display that.

Would looking at that exhibit help you explain what the Internet is? It should come up on the screen to your right.

THE COURT: Do you have any objection to 101?

MR. KLEIN: No, Your Honor. We can't see it on our screens.

THE COURT: Nobody can. Exhibit 101 is admitted and can be displayed.

(Government Exhibit 101 admitted.)

MR. FRIEDMAN: Thank you, Your Honor.

(Pause in proceedings.)

THE COURT: This is not a good start. Why don't we come back to it?

MR. FRIEDMAN: Your Honor, I have hard copies of all these exhibits, so I'll switch to the document camera. They won't be in color nicely, but that should work.

Your Honor, may I publish?

THE COURT: Yes.

Q. (By Mr. Friedman) Okay. Mr. Schuster, can you see that exhibit?

A. I can.

Q. Does this help you explain what the Internet is?

A. It does.

Q. And would you do that for us?

A. I will.

So the middle computers are routers or switches that sit up, and they are considered the core of the Internet. And then the Internet allows companies, home computers --

THE COURT: You don't have a screen?

JUROR: It's not coming up on our screens.

THE CLERK: Let me publish it.

THE COURT: Thank you.

THE WITNESS: I'll start again?

THE COURT: Sure.

A. So the center of this picture is the core of the Internet. The Internet is made up of routers and other devices that route communication and network connections between computers. So your home computer would connect to a router in the Internet, which would then be directed to a company, a website, a service, or otherwise. So that core piece right in the middle that's depicted as a cloud is the core of the Internet.

The devices on each side of that would be -- we call them "end devices," so the user devices or the companies that are then connected to the Internet.

Q. (By Mr. Friedman) And I assume, given what you've just described, it's important for computers to have identities or be able to identify and find each other; is that correct?

A. Those routers in the middle need to understand how to route the communications traffic, yes.

Q. Is there a term or thing that allows them to do that?

A. Each device is given an IP address, an Internet Protocol address.

Q. I'm going to ask you to look at Exhibit 102, and tell me if that would help you explain what an IP address is?

MR. KLEIN: No objection, Your Honor.

THE COURT: We'll admit all these, Exhibits 101 through 110 for now. But 102 is admitted into evidence, and you can display and publish it.

(Government's Exhibits 102 through 110 admitted.)

Q. (By Mr. Friedman) What does Exhibit 102 show?

A. So this is a comparison between an IP address, one that is assigned to a computer, and then comparing that to a physical address, like a home.

So each computer has an address, which is four numbers that are separated by periods, and that tells the routers how to direct the traffic between two computers that sit, potentially, on opposite ends of the Internet. Very, very similar to your home address, where each home address has to have a street number, a street name, a town in order to route postal traffic. So the Internet works in a very, very similar way using IP addresses.

Q. And "IP address" stands for Internet Protocol address?

A. Internet Protocol address, yes.

Q. People use the abbreviation?

A. Almost always.

Q. Going back 20 years to when you were at Cornell, in that era, how did large institutions, companies, how did they handle their need for computing power?

A. Up until recently, almost all companies would have to build their own data centers. So a data center could be an entire floor of a building, or sometimes an entire building, and in there they would put large computers called "servers." They'd put a large number of them in storage components, and they would have to make sure they had appropriate cooling and power.

And, of course, all the networks that went into a facility is called a "data center." And then you had people that would maintain the data center and make sure that the devices were protected and they were running appropriately and they stayed cooled and otherwise.

So they had to build all of those facilities, including the buildings themselves.

Q. Has AWS taken advantage of the Internet to change the way much of the world deals with this now?

A. We have. AWS is considered a cloud provider. So clouds are what takes advantage of the Internet.

Q. Okay. And so what service does AWS provide, or how does it provide it?

A. We provide infrastructure and services called "cloud services" that allow companies that would typically have to build their own computer data centers, we allow them to rent or use or lease computers in our data centers. So, essentially, they don't have to build all of those other facilities themselves on their premises. They can, actually, rent ours.

Q. Did AWS invent this idea or concept?

A. I don't think we invented it, but we were certainly one of the earlier companies to offer these services.

Q. Are you now one of the bigger companies to do that?

A. We are one of the bigger companies offering the service.

Q. Now, this is often called "cloud computing," you said?

A. It is.

Q. Fair to say computers are not suspended overhead in clouds?

A. They're not.

Q. Where are the computers actually?

A. For AWS, they're located at -- we call them "regions." They're located at various geographic areas around the planet.

Q. Okay. Have you looked at a list before this -- before testifying -- of AWS's regions?

A. I have.

Q. Would you look at Exhibit 913 and tell me if you recognize that?

A. I do. It's a list of our regions.

MR. FRIEDMAN: Government offers Exhibit 913.

THE COURT: Any objection to 913?

MR. KLEIN: No, Your Honor.

THE COURT: Okay. 913 is admitted in evidence and can be displayed and published.

(Government Exhibit 913 admitted.)

Q. (By Mr. Friedman) So can you tell us what is the left-hand column and one what is center column here?

A. So the left-hand column is our designation for a region, so where we have a set of data centers that customers can use.

The middle column, the name is just a name that we've also assigned to them, and then the location of those regions.

Q. So many in the U.S.

A. Many in the U.S.

Q. But many in other places, also?

A. Correct.

Q. If you're providing cloud computing services out of these locations, do customers rent a specific large computer or server from you?

A. No. They rent what is, essentially, a virtual machine or a copy or an image that they would use, so a slice of a large computer.

Q. Why do you call it a "virtual machine"?

A. Because it's not, actually, a full computer, as we think about the hardware associated with it. It looks like one from the outside, but it, actually, there are multiple virtual computers that run on any given piece of hardware, the computer itself.

Q. Okay. You've looked at Exhibit 103 before testifying; is that correct?

A. I have.

THE COURT: Any objection to 103, counsel?

MR. KLEIN: No, Your Honor.

(Government Exhibit 103 admitted.)

THE COURT: I'm going to assume -- just go ahead and publish it. If you have an objection, let me know.

Q. (By Mr. Friedman) Mr. Schuster, does this help explain what you've just been speaking about, about virtual servers?

A. It does.

Q. Can you do that for us?

A. So on the left side, imagine a very, very large computer, so something significantly bigger than what you might have at home or your laptop or otherwise. These are very, very large computers.

Because they're so large, we can actually run smaller computers within that same piece of very large hardware computer. And those are called "virtual machines" or "virtual images."

So you can decide what type of computer you want to run on your behalf, all housed in that one physical server.

Q. This is labeled "hypervisor," and there is a label "hypervisor" on there. Can you explain what a hypervisor is?

A. The hypervisor is, kind of, the brain of the physical computer. So it keeps track of how many virtual computers are running on it, who owns those computers, who is leasing those computers, what the configuration of those computers are. It actually helps isolate those computers so they are assigned to a specific customer.

Q. And then when we look at right-hand side, are those some of virtual computers on the physical computer in this example?

A. They are, and they're also examples of AWS services.

Q. So the top two are labeled "EC2 instance." What does that stand for?

A. EC2 stands for "Elastic Compute Cloud." And so it is Amazon's service, or AWS's service, to do the computing part of the computer. So computers have both a computing part and a storage part. This part is the computing part.

Q. You said it stands for "Elastic Compute Cloud"?

A. It does.

Q. Does "elastic" refer to the fact these are scalable?

A. Scalable, you can grow them, you can get rid of them, you can include more, you can grow as the business grows, so it's scalable, yes.

Q. And I also see the word "instance." What does "instance" mean?

A. Instance would be one -- one virtual computer is considered an instance of EC2.

Q. Is that largely an Amazon term?

A. Yeah, but I think it's more widely adopted as well now.

Q. Okay. And then at the bottom we have something that does not have a screen and is labeled "S3 bucket" --

A. Uh-huh.

Q. -- to what does that refer?

A. So much like I said, when you think about computing, there's the computing side and then the storage side. "S3 bucket" stands for "Simple Storage Service." Basically, you can think about it as a hard drive or a place to store files, images, anything you want to store up into the cloud.

Q. And you've looked at Exhibit 104 before testifying?

A. I have.

Q. Would that help you explain the concept of a bucket?

A. Yes.

MR. FRIEDMAN: Offering Government Exhibit 104.

MR. KLEIN: No objection.

THE COURT: 104 is admitted and can be displayed.

(Government Exhibit 104 admitted.)

Q. (By Mr. Friedman) Can you explain how this amplifies your description of what a bucket is?

A. Sure.

So a "bucket" is just a very, very generic term that we use, because we can store all kinds of things, all kinds of digital objects. Any digital object that can be stored on a computer can be stored in a bucket.

So much like on the right side, where it might be a filing cabinet, where you think about storing documents that are in folders and in drawers, you can, actually, replicate that in a bucket, or you can store all of your pictures, or you can store configurations for computers that you want. Anything that is on a computer can be stored in an S3 bucket. So it's just a place to store things.

Q. If we go back to the previous exhibit, the hypervisor, there is a reference at the bottom to something called the Instance Metadata Service?

A. So Instance Metadata Service is -- it's tightly coupled or it's associated with a hypervisor, but it stores information about the virtual instances on the right-hand side of this diagram.

So, for example, in an EC2 instance, that instance would have a name, that instance would have a customer who owns or is using that instance, or renting that instance. It would have information, like the IP address, on how to connect to that instance.

So it is specific information about what's running on the piece of hardware on the left-hand side.

Q. Okay. Are you familiar with the concept of "credentials"?

A. I am.

Q. What are credentials, in general?

A. Credentials are, basically, you think about logging into your company computer or your home computer, it's an identity, it's who you are. And then there's this authentication piece. So lots of times, it is a password, is probably the easiest way to think about it.

Credentials are the identity and the password coupled together.

Q. Okay. And the credential stored on the Instance Metadata Service, for what would that information...?

A. That information stores role information for the instance.

Q. Okay. And for the instances that are on the --

A. On the physical server, correct.

THE WITNESS: I'm sorry. Excuse me. Can I get a glass or a cup?

THE COURT: Sure. Glasses are out; cups are in.

THE WITNESS: Thank you.

THE COURT: Sure.

Q. (By Mr. Friedman) When one of the instances shown on this diagram needs information to run, where does it get that information?

A. It would make a request or query the Instance Metadata Service.

Q. And is the Instance Metadata Service something that is generally available to the public? Can I log in from my home computer?

A. You cannot. It is part of the core Amazon services.

Q. Who can make a call to the Instance Metadata Service, or communicate with it?

A. People that are authorized and running on the instances that are on that computer.

Q. Okay. So internal to that computer?

A. Internal to that computer, correct.

Q. And people who are not, are they able to communicate with it?

A. They're not supposed to, no.

Q. Are you familiar with something called the shared security model?

A. I am.

Q. What is the shared security model?

A. It's a way for us to describe what AWS is responsible for in securing a company's services and what the customer is responsible for securing. It allows us to be very clear about what we will secure and respond to, and then what the customer needs to.

Q. Okay. So let's start with AWS. What is AWS responsible for securing?

A. So continuing to use this picture, AWS would be responsible for the physical data centers, so the perimeter: the fences, the facility itself, who goes into and comes out of those data centers.

AWS is also responsible for the hardware that's running in those data centers and making sure that the services that are on the hardware runs as expected so there are no bugs.

Q. And what is the AWS customer or client responsible for?

A. They're, basically, responsible for any application that runs on the instance. So, basically, the hypervisor. We call it "up." So they would take, like, an EC2 instance and say they wanted to run a web server on that. They would be responsible for the application of the web server, the security of how it's configured, who can log into, who can use it, and their credentials for that.

Q. Does AWS sometimes use an analogy of "something up, something down"?

A. We do. It's not just AWS.

Q. Can you explain that one to us?

A. Sure.

It's a logical representation for computers. So the very, very bottom is the physical data center. That would be called "layer one." And then above that would be the hardware, and above that would be the controller of the hardware, and above that would be, like, the virtual instance. Then that's where we would stop.

And then on that would be how the computer, what applications are installed on the virtual instance, and then above that would be the credentials that could be used, and how the credentials are distributed and used.

Q. Okay. And the customer or client is responsible for that?

A. Correct.

Q. Are you familiar with some of the ways in which AWS clients protect their information in their servers?

A. I am.

Q. Is one of those something called a "firewall"?

A. It is.

Q. Would Exhibit 105 -- you've looked at that before -- help explain what a firewall is?

A. Yes.

THE COURT: 105 is admitted into evidence.

MR. KLEIN: No objection, Your Honor.

(Government Exhibit 105 admitted.)

Q. (By Mr. Friedman) So what, in general terms, is a firewall?

A. So a firewall, essentially, is a gate or a gatekeeper to determine what computers can connect. So a firewall is thought of a front side of the firewall and the back side of the firewall. The back side of the firewall represented in the cloud here on the right-hand side are all the devices behind the firewall that the firewall is protecting.

So the firewall is, essentially, a gate that controls what computers can come and access those devices that sit behind it that it's protecting, and who is allowed to do that.

Q. Okay. Is it fair to say it directs and monitors traffic?

A. Yes.

Q. Does a firewall allow all the traffic to pass through?

A. Typically, no.

Q. How does a firewall know what to do?

A. The firewall is configured with rules. We talked about IP addresses earlier. So a simple rule would be, this one IP address is able to connect to every device that passes here, or I might be able to say this one IP address can connect to no computers that sit behind it. So it controls that. It's a configuration.

Q. Are there also more complicated rules?

A. Oh, absolutely.

Q. Does Amazon design and supply firewalls to customers?

A. We do.

Q. Do all customers use the AWS firewalls?

A. No.

Q. What do customers who do not use AWS firewalls do?

A. If they have a firewall -- and, again, that's entirely their decision -- they would install their own. It would be one of the applications that would be installed on one of those EC2 instances.

Q. Are you familiar with whether Capital One generally used AWS firewalls or its own firewalls?

A. They use their own.

Q. Is that something that's typical, or, at least, many companies do?

A. Many companies do that, yes.

Q. Is another way in which customers can protect information related to something called the instant Identity and Access Management, or IAM system?

A. It is.

Q. What is the IAM system?

A. The Identity and Access Management system is a way for customers to configure which accounts can do certain things. It, basically, aligns a user with a set of services and what they're allowed to do, based on their log-ins.

Q. Does it allow a user to break out and provide certain people certain accesses and other people different accesses to control that?

A. It can, yes.

Q. And why would it want to do that?

A. They want to do it based on the business. So there will be some services that businesses decide need broader access, and some areas of their company, some services or data stores or others, where they may decide nobody should have access, or a very limited number of people should have access to.

Q. Let's imagine a company with 1,000 employees. If they want the CEO to be able to see certain information but the front-desk person not to, is that something that IAM could --

A. IAM could absolutely be used for that, yes.

Q. And how, in general terms, would it be used for that?

A. So they would -- each account has a name and an authentication, like we said earlier. And then the customer would assign permissions to that account. So for the CEO, they may just say the CEO with this log-in and these credentials can do anything -- if permitted, anything in the company they can access and do, where maybe that front-desk person, you would say with these credentials that was aligned with this person, they have very limited to no access or use of services within there. So it runs the range.

Q. When a client signs up or opens an account with AWS, what do they started with in terms of accounts?

A. They start with a log-in and a password. They have nothing else associated with that account.

Q. Are you familiar with term "root account"?

A. Root account, yes.

Q. Is what you're describing the root account --

A. It is the first account, the root account that can do anything within that account, yes.

Q. And what advice does AWS give people about what to do when you've just started and been given a root account?

A. We typically advise that you should never use that root account. So we advise users to take that root account, and then create sub-accounts under there with more limited or more restrictions, limited access, and then never use the root account again.

Q. Okay. And can the accounts -- the sub-accounts you're talking about, can they be assigned to different people?

A. Yes.

Q. Okay. Have you looked at Exhibit 106 and would it help you explain this and the next subject we're going to talk about?

A. Yes.

MR. FRIEDMAN: Government's Exhibit 106.

THE COURT: Any objection to 106, counsel?

MR. KLEIN: No, Your Honor.

THE COURT: 106 is admitted into evidence and can be displayed.

MR. FRIEDMAN: Thank you, Your Honor.

(Government Exhibit 106 admitted.)

Q. (By Mr. Friedman) Is what you're talking about the left side of this diagram?

A. It is; typically, user accounts, yes.

Q. What is a user account?

A. A user account is somebody who would sign up for a service or be allocated an account. It would come with a user name and, typically, some way to prove that you are the user who you claim to be. Lots of times it's a password.

Q. When you talk about "password," you're talking about that is a form of credential; is that correct?

A. It is a form of credential, yes.

Q. And this lists two other things, "key" and "token"?

A. Right.

Q. What are those?

A. They're just stronger -- stronger ways to do authentication.

Q. Who decides who gets a user account?

A. The customer.

Q. Not AWS?

A. Not AWS.

Q. And in your experience, to what types of people are user accounts generally assigned?

A. Typically within the business, so for a large customer, a customer would have several accounts, and they would then assign those accounts to their employees.

Q. Are user accounts generally assigned to members of the public or people not associated with the client?

A. Outside the customer --

MR. KLEIN: Objection, Your Honor; calls for speculation.

THE COURT: Just in your general understanding. You can answer.

Overruled.

A. Typically not, no.

Q. (By Mr. Friedman) Say someone is assigned a user account. Does a user account start with any permission to do anything?

A. If it's just a blank user account, no.

Q. How does a person with user account get permission to do things?

A. The owner of the account who is setting up the user account would then assign permissions to that and what they're allowed to do, based on their needs.

Q. What types of things might these permissions be?

A. What services they can use in AWS, what resources they can access, what data stores they can access.

So thinking about our previous example, they could be assigned to use EC2 to launch or create new EC2 instances. They might also be able to access or not access buckets, S3 buckets that we talked about earlier.

Q. Are you familiar with something called "the principle of least privilege"?

A. I am.

Q. What is that?

A. It's a way to think about how to only assign permissions that are absolutely required to do the job for that account.

Q. And why is that a principle that people talk about in the computer-security business?

A. It prevents the potential for abuse, if an account were to be compromised or lost or otherwise.

Q. Is it a little like need to know --

A. Need to know, uh-huh.

Q. Who decides what permissions a user account receives?

A. The customer or the account owner.

Q. Not AWS?

A. Not AWS.

Q. Now, that was the left-hand side of this chart. The right-hand side seems to refer to something called a "role." What is a role?

A. So a role is another way to assign permissions. So where, on the left side, the user account might be assigned to a person, we also have a way to define groups of permissions or roles.

So, for example, many employees in companies might wear multiple hats. So an employee might be part of the finance department, but also might be part of an audit department or otherwise. And so a role is a way to collect like permissions. So you can say if you are part of the finance department, you have permissions to access financial data, financial services, et cetera, when you have that role.

Q. Okay. Why does it make sense to have that functionality or that ability built into the system?

A. It's much easier to configure correctly. So, for example, customers are able to think very concisely about what they want, say, the financial people to be able to do, and then that can be assigned to the users.

If we didn't have that, companies would have to think, perhaps, about millions or thousands of users, and then think about what department they're in, what access do they need. It would be higher prone to error.

Q. Okay. This diagram depicts a couple people next to the role and a couple of computers or servers. Why is that?

A. So role -- people can assume a role. So the example I used was the finance department or a person assigned to the finance department. But also computers can be assigned a role.

And so, for example, a computer can say I need to be able to access, say, an S3 budget to understand what my configuration should be, what rules I should run under, or things like that. And so they can assume a role to be able to access a specific bucket for data that the computer needs to know and how to run.

Q. When a customer creates a role, does it start with any permissions or powers?

A. It does not.

Q. How does it get permissions or powers?

A. The customer or account owner who created the role assigns permission within that role.

Q. And is that similar to the permissions we talked about for user names and user accounts?

A. Yes.

Q. In your experience, for whom are roles generally created?

A. Roles are typically created for people that have accounts within a company. And so for a large company, they would understand all of their accounts that are within the company domain, assigned to employees, and the computers they use, and then they would think about assigning to those groups of people.

Q. In your experience, are roles generally available or assumable for members of the public not connected to a client?

MR. KLEIN: Objection, Your Honor; calls for speculation.

THE COURT: In his experience. He's not speculating. He's giving his response on his experience.

The objection is overruled. Go ahead.

A. Typically not.

Q. (By Mr. Friedman) So down below that, we see the term "role name." What is a role name?

A. It's just an identifier for that role.

Q. Okay. Selected by the client?

A. Yeah, selected by the client, yes.

Q. And then it says "temporary credential," whereas user account said "permanent credential." What does temporary credential mean?

A. What it means is a credential is created only while that role is being used. So, for example, on the left-hand side, when you have an account, those are longer-term credentials, so those typically do not change. So if that password were to be lost or otherwise, you'd have to change it all, and there might be a risk.

Temporary credentials allow them to be used just one time or for a very limited state, and so they can't be used again.

Q. And so what does someone who is trying to assume that role have to do if they want to do their work tomorrow?

A. They would have to query the metadata service and get a new -- and assume that role to get a new, temporary credential.

Q. And the credentials listed here are slightly different from those for user accounts.

A. It is.

Q. Can you tell us why that is and what these terms mean?

A. Because you're not actually authenticating, and you're assuming that role, it -- a temporary credential is made up of the access key that was used. The secret key -- so an access key is just the one-time key -- the secret key assigned to it, and that's all rolled together as the token that's then presented to the service.

Q. Is the access key sometimes called a "session key"?

A. It is. It can be called a session key.

Q. Is there a separate term sometimes used for secret access key?

A. Not that I'm aware of. We just call it a "secret key."

Q. Can an individual assume a role without having one of the security credentials or multiple of the security credentials listed here?

A. They should not.

Q. And so what does the use of credentials for roles allow the clients to do?

A. Ask that one more time, please.

Q. By requiring the use of credentials for a role, what does that allow customers to do?

A. It allows customers to clearly define who should be part of that role -- who has the ability to use that role. So because you're using the user name and then credentials that are assigned to that person, you have some assurances that that person is who they say they are, and then, consequently, can assume that role.

Q. Let's go back to Exhibit 103, if we could.

Say one of the instances, one of the virtual servers needs to assume a role to do something, how does the instance get that information and assume that role?

A. So the instance would ask or query the Instance Metadata Service and ask for what roles are available to it, and then would be able to choose which role to assume.

Q. Okay. Does the Instance Metadata Service provide that information --

A. It does.

Q. -- and then the credential?

A. And then the session credential as well, yes.

Q. You talked earlier about who could access instances, and if I remember correctly, you said the only people who can access the Instance Metadata Service are within that hypervisor or that group of virtual servers?

A. Yes, correct.

Q. Does that affect who is able to access the Instance Metadata Service to get credentials?

A. It does.

Q. Who is able to do that?

A. The people who are authorized to access the instance itself; so log into the instance and use the instance.

Q. If an external source were to ask for that information about roles, would the Instance Metadata Service provide it to that external source?

A. You can't connect to the Instance Metadata Service from the outside. So I can't just try to connect to the Instance Metadata Service directly from a computer not in AWS or not in that account.

Q. Okay. So that shouldn't even be possible?

A. Should not even be possible.

MR. FRIEDMAN: Your Honor, I'm about to change topics. I'm happy to do that or --

THE COURT: No, keep going.

Q. (By Mr. Friedman) Mr. Schuster, are you familiar with an incident that occurred in July of 2019?

A. I am.

Q. And did that start out as a breach of at least one AWS client?

A. Yes.

Q. How did AWS first learn about this?

A. A leader in Capital One connected to one of our leaders in AWS.

Q. To whom did he connect?

A. To Steve Schmidt, our chief information security officer.

Q. Is he your boss?

A. To my boss.

Q. Did you hear about this pretty quickly?

A. Pretty quickly.

Q. From that point on, what was your involvement?

A. Part of my team supported Capital One.

Q. Okay. Were you yourself kind of involved and abreast of what happened over the next few days?

A. I was the escalation point, so I ensured that Capital One had the resources they needed. We were answering the questions that they needed, and, if not, I was the one that got called for more support or otherwise. But it was my team that was most directly -- people on my team that were most directly involved.

Q. Under the shared responsibility model, did responsibility for this end up on one side or the other, and did that affect what you did?

A. It did end up on one side or the other. The responsibility for this ended up on Capital One's side of that shared security model. We still supported them, we still gave them permissions they needed, but it allowed us to not take actions that we might otherwise had needed to take.

Q. Did you take some actions, though?

A. I did.

Q. What did you do?

A. So when we first became aware of it, our first responsibility is to ensure that this wasn't a problem in our services. If it was a bug or a problem in our services, I would have to fix that very quickly, because other companies could, potentially, be implicated or involved or have a similar risk. And so we needed to determine whether this was an error on our side of the shared security model or not.

Once we determined that, then I was -- then we were just -- we directly supported Capital One as to their needs.

Q. In general terms, how did you determine that this was on the Capital One rather than the AWS side?

A. We were able to look at the data that Capital One provided us, and they were already pretty well down the path of understanding what the errors were. But we still checked into our services.

Q. When you talk about data they provided, in general terms, what type of data is that?

A. In general terms, log data.

Q. Okay. What is a log?

A. A log is a computer audit, a computer -- it's -- each line in a log file tells you who did what and what did they do and when they did it on a computer. And so in looking at log files, you're able to construct what happened and who was doing it and what services were used.

Q. So this is probably not a great example, but we always read about black boxes on airplanes that record every event that's happened. Is this similar for a computer?

A. It's not a bad example, yes.

Q. When AWS looked at the logs -- is there a particular type of logs or a name for the logs that you were looking at?

A. We have a service called CloudTrail, so they were CloudTrail logs.

Q. When AWS looked at the cloud trail logs, what did you generally determine?

A. We determined that the firewall was used as a way to get access to data, and then we were also able to confirm the role that was used to access the buckets that contained the data.

Q. You said that you determined that a role was used to do this?

A. Yes.

Q. Were you able to determine whether that use of role was intended or authorized or whether it was not, or was that beyond the scope of what you did?

MR. KLEIN: Objection, Your Honor; calls for a legal conclusion.

THE COURT: Well, first answer the question. Was it beyond the scope of what you did?

THE WITNESS: It was not beyond the scope of what I did.

THE COURT: And did you actually do what Mr. Friedman's question asked, then?

THE WITNESS: We actually worked with Capital One to confirm that the role was used. And then -- I can't speculate on why that role was used and set up the way that it was.

THE COURT: Okay.

THE WITNESS: That was beyond the scope on our intention.

THE COURT: Thank you.

Q. (By Mr. Friedman) But you determined that a role was used?

A. I determined that a role was used and what role was used, yes.

Q. And does that necessarily resolve the question of whether that was a legitimate and authorized use or not a legitimate and authorized use, or does that leave that open?

MR. KLEIN: Objection, Your Honor; same; calls for speculation.

THE COURT: Overruled. You can answer.

A. It leaves it open.

Q. (By Mr. Friedman) Do you have a general understanding of how the access in this case, the breach, took place?

A. I do.

Q. And have you looked at Exhibit 107, and would that help you explain?

A. It probably would, yes.

MR. FRIEDMAN: Government offers Exhibit 107.

MR. KLEIN: No objection, Your Honor.

THE COURT: 107 is admitted and can be displayed.

(Government Exhibit 107 admitted.)

Q. (By Mr. Friedman) Mr. Schuster, using this exhibit, what understanding did you develop of what happened?

A. Okay. So the first step, the -- I'll walk through this very quickly.

The left side is the computer that was used by the attacker to get access to the logs -- or to the files themselves.

So the very first step that that computer would have done was scanned or looked for a specific configuration of that firewall that could potentially be exploited.

Q. Okay. So the computer communicated with the firewall?

A. The computer, yeah, communicated with the firewall, and then connected to it.

The second step was, once they were able to look for that configuration of the firewall, they were then able to trick that firewall into querying the Instance Metadata Service to give up -- to give role credentials that could be assumed by the firewall.

Q. Okay.

A. The third step is that, once the role credentials were obtained and then passed through the firewall to the attacker, then that firewall passed those role credentials back to the attacker. And then from there, the attacker was able to use those credentials to access the S3 buckets.

Q. Could that outside computer have communicated directly with the Instance Metadata Service to get this information?

A. No.

Q. And why is that?

A. There are security controls in place that requires only instances running on the hardware to query the Instance Metadata

Service.

Q. Okay. You used the word "trick" a moment ago. Why did you use that?

A. Because the firewall wasn't set up -- the firewall was misconfigured. It wasn't set up to pass requests from an outside person to the Instance Metadata Service.

Q. Okay. And so why did the Instance Metadata Service respond to the request?

A. Because it thought that the request was coming from the firewall -- by the firewall.

Q. You talked about the fact that this resulted in the credentials going to the outside computer, correct?

A. Yes.

Q. Does Exhibit 108 help you show what that computer was able to do once it had those credentials?

A. Yes.

MR. FRIEDMAN: Government offers Exhibit 108.

MR. KLEIN: No objection, Your Honor.

THE COURT: 108 is admitted in evidence and can be displayed.

(Government Exhibit 108 admitted.)

Q. (By Mr. Friedman) What does Exhibit 108 show?

A. So Exhibit 108, the bottom little cloud in the larger cloud is what we were looking at within AWS. That includes the firewall and the EC2 instances.

Once the role credentials were passed to the attacker way on the left, they were able to use -- Amazon has an access point called the "Command Line Interface," so it's a way to program the way Amazon functions. They were able to use that role to then query our S3 service to get access to the buckets.

Q. You said "AWS CLI" stands for "Command Line Interface"?

A. Yes.

Q. Is that one of many multiple gateways into Amazon?

A. One of the few, yes.

Q. Is it a significant one, though?

A. It is a significant one, yes.

Q. Once the attacker used the credentials to go through the command line interface, what was the attacker able to do inside Amazon Web Services?

A. They were able to query what S3 buckets were available for that role, and they were also able to determine the permissions associated with those buckets that were visible to that role.

Q. Were they able to see S3 buckets that were not within that role's permission?

A. No.

Q. And would they have been able to look inside buckets that -- inside which buckets could they look?

A. They were allowed -- it's a little bit tricky.

The role, actually, allowed to look at all S3 buckets, but the buckets themselves were configured more securely. So the role itself did not prevent, but the buckets themselves prevented some access and some listing of contents.

Q. I meant to ask you a slightly earlier question.

At what universe of buckets could the attacker look?

A. The subset of the buckets that had both the permissions from that role or within that role, and the buckets that allowed access.

Q. Okay. All AWS clients?

A. No, Capital One clients --

Q. Okay --

A. Or Capital One buckets.

Q. Got it.

And you said the role had permission to look at certain buckets?

A. Yes.

Q. But buckets could also have permissions?

A. They could, yes.

Q. And so what would the impact be if buckets had additional permissions?

A. So if buckets had additional permissions -- a bucket can be configured to not list the contents, not show what's in the bucket, based opinion the account that's looking at it or the role that's being used to look at it. So a bucket actually controls its -- can control its own permissions as well.

Q. And there is also a line to something marked as "EC2 instances"?

A. Yes.

Q. Why is that there?

A. Because the AWS CLI can also access EC2 instances as well.

Q. And would the role's permission determine what the attacker could do with respect to EC2 instances?

A. Yes.

Q. And can you explain how that is?

A. When you create a role, you create explicit permissions that are allowed, and also explicit permissions that are denied within that role. So when you assume that role, it controls what services you can use, what data you can access, what buckets you can access or otherwise.

So absolutely, depending on the permissions assigned to that role, controls what you can do.

Q. Okay. Are you aware of where within the United States Capital One has data centers?

A. Generally, yes.

Q. I think I asked that incorrectly.

Are you aware of where AWS has its data centers?

A. I am.

Q. And are you aware, generally, of which of those data centers Capital One's information is stored at?

A. Generally, yes.

Q. Can you tell us?

A. Typically, in Virginia and on the West Coast, which is in Oregon.

Q. Looking back at Exhibit 913, does AWS have any data centers within the state of Washington?

A. No.

Q. So if someone within the state of Washington sends a command to get information from Capital One S3 buckets, would that command have to necessarily travel to another state?

A. Yes.

THE COURT: Is this a good place to break?

MR. FRIEDMAN: Perfect, Your Honor. Thank you.

THE COURT: We're going to break for lunch. You can go to lunch anywhere you want with whoever you want, just don't talk about the case. And, please, I'm going to send you right out. Please have everybody stay to allow the jurors to get to the elevators first.

And then at 1:20, please be back in Judge Pechman's courtroom, and Victoria will bring you up to start about 1:30. Okay? Leave your notepads and pens on your chairs.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Approximately how much more do you have, Mr. Friedman?

MR. FRIEDMAN: With Mr. Schuster, I'm two-thirds of the way through, Your Honor.

THE COURT: Okay. And then, obviously, Mr. Klein, you're doing cross-examination?

How about Kat Valentine; who is doing cross on that?

MR. FRIEDMAN: I am, Your Honor.

THE COURT: I'm not sure we'll get there, but Mike Fisk?

MR. HAMOUDI: I'm doing Mike Fisk, Your Honor.

THE COURT: Okay. Take that list that you got, and just put down who is doing the objections and the cross.

MR. KLEIN: I'll do that.

THE COURT: Take a look at Exhibits -- are you in the 100s, for the most part, with this witness?

MR. FRIEDMAN: I think there is a couple others, but we talked about it.

MR. KLEIN: Yes, Your Honor.

THE COURT: If you know you're not going to have any objection to these exhibits, let's just move them into evidence now.

MR. KLEIN: We'll talk about that at the break, Your Honor. This is all I'm aware of at the moment.

THE COURT: Sure.

I'll ask everybody to be ready to go here at 1:30. You see that it takes time to get the jurors up from 14. If I shoot for 1:20 with them, we should be able to start at 1:30.

MR. HAMOUDI: Did you ask who was doing cross for

Fisk?

THE COURT: Just send an email.

MR. HAMOUDI: I understand.

THE COURT: Great. We're adjourned.

(Court in recess 12:10 p.m. to 1:33 p.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Please be seated.

So we'll continue with the testimony of Mr. Schuster.

And I just walked a little bit around up to Whole Foods, and I think I saw about 15 people with AWS backpacks or sweatshirts, so the army is out there.

THE WITNESS: They are.

THE COURT: And they know you're here.

THE WITNESS: We have a lot of employees here in the city.

THE COURT: Go ahead, Mr. Friedman.

MR. FRIEDMAN: Thank you, Your Honor.

Q. (By Mr. Friedman) Mr. Schuster, are you aware of something called responsible disclosure?

A. I am.

Q. What is responsible disclosure?

A. The objective of responsible disclosure is when somebody finds a security issue, either in a service or with a company, a configuration error, or a bug, they report that to the one --

those that are responsible for fixing it, and then work closely to make sure that all parties understand so we reach a conclusion where the issue is fixed.

Q. Okay. Do companies have response -- does this happen generally or do companies have responsible disclosure programs?

A. Some companies have formal responsibility disclosure programs, others do not. But there are still ways to connect with their security team and still disclose responsibly.

Q. Does AWS have a formal responsible disclosure program?

A. We do.

Q. Okay. How would you go about -- say you had information you wanted to report to AWS, how would you go about finding that program?

A. There's actually lots of ways to -- to report security issues. I have a security mailbox that's easily searchable, my response team does, that's triaged. Some come through customer support. There's lots of ways to report a security issue which then ultimately comes to my team.

Q. If you Google AWS responsible disclosure, would you find a site or link?

A. Yes.

Q. Okay. And does AWS's responsible disclosure program offer payments to individuals in any circumstances?

A. Sometimes, yes.

Q. When would AWS pay somebody who made a responsible disclosure?

A. It depends on how they disclose it. The severity of the issue, the creativity of the issue. We would go through a triage process.

Q. Okay. Would you take a look at Exhibit 954 and tell me if you recognize that?

A. Sorry, I have to put my glasses on.

Q. Sorry about that.

A. Yes, that's our disclosure.

MR. FRIEDMAN: Government offers Exhibit 954.

THE COURT: Any objection?

MR. KLEIN: No objection.

THE COURT: 954 is admitted and can be displayed to the impatient jury.

(Government Exhibit 954 admitted.)

Q. (By Mr. Friedman) Okay. This is the web page describing Amazon's responsible disclosure program

A. It is.

Q. And if we -- does this page also authorize Amazon customers to do anything?

And let's zoom in, the Reporting Suspected Vulnerabilities section.

A. Right.

So Amazon customers can test the configuration of their use of our services. So as we discussed earlier, applications that run on our services, the configuration of those applications, they can for themselves or they can even contract with a company who would do testing against how those services are configured to make sure they're done securely.

Q. When it says Amazon AWS customers are welcome to carry out security assessments against their infrastructure, what's a security assessment?

A. It's -- typically, there are tools that are available to do scanning, tests for certain vulnerabilities, tests for configurations to make sure that everything is according to secure practices.

Q. And when it says they're authorized to conduct penetration tests against the AWS infrastructure, what are penetration tests?

A. Penetration tests go beyond simple tooling. Penetration tests will actually be somewhat more aggressive and actually try to break in, where some of the other tools will just test and flag if there are potential configuration errors. Penetration tests will actually try to take steps to actually break in.

Q. Okay. So this authorized AWS customers to do that against their own accounts and information?

A. Correct.

Q. What about can customer A try penetration testing on customer B's account?

A. No, no.

Q. Okay. Does Amazon authorize or allow that?

A. No.

Q. What about members of the public?

A. No.

Q. Are you aware of a handwritten note passed to an Amazon employee in May of 2019?

A. I am.

Q. Would you take a look at Exhibit 952 and tell me if you recognize that?

A. I do.

Q. Is that the note?

THE COURT: 952, any objection?

MR. KLEIN: Your Honor, we don't because the government's going to call another witness.

THE COURT: All I want is do you object to it being shown to the jury now, yes or no.

MR. KLEIN: No, Your Honor.

THE COURT: Okay. 952 is admitted into evidence and can be displayed.

(Government Exhibit 952 admitted.)

Q. (By Mr. Friedman) Is this the note, Mr. Schuster?

A. Yes.

Q. Do you have an understanding of when this note -- or when and where this note was passed to an Amazon employee?

A. I do.

Q. And what's that understanding?

A. It was passed to an Amazon employee, an Amazon security leader. I believe he's at a conference. Was passed to him by an unknown individual in May.

Q. Okay.

A. Late May.

THE COURT: May of what year?

THE WITNESS: I'm sorry, 20 --

THE COURT: 19.

THE WITNESS: '19, yes, sir. Thank you.

THE COURT: Okay.

Q. (By Mr. Friedman) Does Amazon have an understanding of who handed this note to an Amazon employee?

A. We do not.

Q. I want to talk about the contents of this note for a moment.

There's really three lines; correct?

A. Yes.

Q. What is the middle line?

A. The middle line is the IP address. As we talked about earlier, the address of the computer, the identification of the address of that computer.

Q. Okay. And I should ask you one question I forgot to ask. You said it was passed in May of 2019?

A. Yes.

Q. Do you have an understanding of how that relates in time to when Capital One's data was taken?

A. So I believe Capital One's data was taken at the end of March of the same year, 2019.

Q. So --

A. -- passed in May.

Q. Roughly two months later?

A. Multiple months later.

Q. Okay. You said the middle line is an IP address?

A. Yes.

Q. Okay. The -- do you know whose IP -- what did Capital One -- I'm sorry, what did Amazon -- or AWS do with this note?

A. So when this was passed to my instance response team, we looked up the IP address to determine which customer had that IP address. So we were able to then determine that that IP address was being used by Capital One.

Q. Okay. And so what did Amazon do once it determined that?

A. We reached out to Capital One to tell them that we had information that they might want to look into.

Q. Okay. Did Amazon give a copy of the note to Capital One?

A. I think we gave an image of the note, yes.

Q. Fair enough.

Okay. The top line, can you tell us what that says?

A. It says open SOCKS proxy.

Q. And what is -- what would a open SOCKS proxy -- what does that mean to you?

A. So a SOCKS proxy is a little bit like a firewall, but functions differently. It's meant to bridge -- bridge communication between two computers. It's a service that people can set up to allow two computers to communicate.

Q. Okay. And then what does the bottom line or two lines say?

A. Can hit instant metadata service IMS-lots of security credentials.

Q. Okay. Do you consider this a responsible disclosure?

A. I would not.

Q. Why is that?

A. Multiple reasons. First, there's no timestamp to know exactly what we were looking for or where we were looking for it.

Q. Can you tell us, why is a timestamp important?

A. As we talked about earlier, we talked about logs of servers. When servers are producing logs that tell you what happened, where, and who did it, those are enormous, potentially, depending upon how busy that computer is.

And so at this point, it would have been two months -- March, April, May -- two months after the actual incident happened, so there would have been millions of lines of audit trail to look at backwards to try to figure out what happened, if anything happened. So a timestamp would have allowed you to look at exactly, at least in a window of time, to look to see what was happening to try to understand what this message actually meant.

Q. Okay. Why else do you not consider this to be a responsible disclosure?

A. Second reason is an open SOCKS proxy is actually a misidentification of the resource. Resource was a firewall. And so Capital One -- I don't know what Capital One did. But if it would have come to my incident response team, I would have looked at that IP address, I would have looked and said it was identified as an open SOCKS proxy. I may have concluded -- I don't -- I don't have open -- I don't have SOCKS proxies in my environment, so someone must have reported this out of error. Maybe they got the IP address wrong or otherwise.

Q. So do you believe that this does or does not report the misconfiguration that actually existed?

A. It identifies a proxy.

The other issue -- my third problem with this is on why it's not responsible disclosure is that the issue wasn't that there were security credentials available, the issue was there was a theft of data. And so it -- it actually didn't even identify what the -- what the real risk was.

Q. Okay. Do you have an understanding of whether this was enough for Capital One to figure out the vulnerability that had existed and been exploited?

A. I --

Q. You may or may not know.

A. I don't know and I wouldn't want to speculate.

THE COURT: Thank you. That's the right --

Q. (By Mr. Friedman) Okay. Great.

All right. Ms. Thompson was arrested -- well, you learned of the breach that has led to this case in July of 2019; is that correct?

A. Correct.

Q. Okay. And I think you've told us earlier about steps that Amazon took to cooperate with Capital -- to assist Capital One?

A. Correct.

Q. Did Amazon take -- or did AWS take steps to notify or protect customers other than Capital One?

A. We did.

Q. Okay. Why was that?

A. In short, it was the right thing to do for our customers. If there's a risk that we know about, we will try to help our customers take steps if necessary.

Q. Were you concerned that other customers might have the same misconfiguration and vulnerability?

A. We had data that we concluded, yes.

Q. Okay. Now, is it theoretically possible that a customer would want to configure the firewall the way that the firewall in this case was configured?

A. Theoretically, yes.

Q. Okay. Why might that be the case? Why would a client want to do that?

A. So firewalls, as we discussed, allow traffic -- let you make decisions on traffic that comes in and out. This firewall was also configured as a proxy. A proxy allows the firewall to -- when a -- when a computer is trying to connect to another computer, it can either go directly, so the two computers talk pretty much directly to each other, or a proxy actually does the communication on behalf of the other computer. So it's actually an additional security control that you can put in place that allows the computer that's initiating the call to kind of hide from the other computers. It's additional security control. And so there are reasons for proxies, both forward proxies as well as reverse proxies.

Q. Okay. Would that be -- in your experience, would that be an unusual configuration for a company to implement?

A. For a large financial institution, yes.

Q. Okay. Are you aware personally of any instance in which a significant company or government entity or university has configured their firewall that way?

A. To run also as a proxy?

Q. Yeah.

A. Yes.

Q. Okay. And what -- in that case, what did that allow access to?

A. It can allow access to anything you want it to allow access to. Typically, it's just for protected resources that you want to make available.

Q. To the public?

A. To the public sometimes, yes.

Q. Okay. Would -- in your experience, have those been limited resources, as opposed --

A. Very limited resources and explicitly allowed.

Q. Are there easier ways, if you want to set up to make resources public, to do that than to proxy them through your firewall?

A. Absolutely.

Q. Okay. Are you aware of any instance in which a large Amazon client has set up its firewall deliberately to allow proxy into internal resources and data?

A. I am not.

Q. Did that contribute -- is that one of the reasons Amazon was concerned that other customers might have this configuration or misconfiguration?

A. It is.

Q. Okay. What steps did Amazon take to alert other customers?

A. Well, much like what the scanner -- the attacker did, we created a scanner that looked across our customers specifically looking for this configuration of this firewall to identify if there were other customers that had a similar misconfiguration.

Q. When you built that scanner, did you find other customers with this configuration?

A. We did.

Q. And what did Amazon do once it found those customers?

A. We reached out and notified them.

Q. Okay. Why did you notify each of those customers?

A. Because at this point the -- the issue was more widely known. We were concerned for copycat attackers. Once you know of a security issue, it becomes easier to attack in the same way. And we also wanted to make sure that our customers intentionally configured their firewalls to function that way.

Q. Okay. During the course of this case, did Amazon also receive information about other customers that Ms. Thompson may have accessed their computers?

A. We did.

Q. From whom did you receive that information?

A. We received it directly from Capital One.

Q. Okay. And what did Amazon do with that list of customers?

A. We also reached out to those customers. I believe those customers, we tried to initiate phone calls, as opposed to emails or other types of connection.

Q. To warn them that they appeared to have misconfigured service?

A. Yes.

Q. Prior to the time that Ms. Thompson was arrested, was the combination of configurations, the vulnerability that she exploited, was that widely known?

A. All of the -- all of the steps that were used, no. Each individual step was relatively well-known.

Q. Okay. But prior to that, was -- the ability to combine these steps in order to access internal resources, was that something that was widely known?

A. It was not widely known.

Q. Were you aware of any instance in which any hacker had done that before Ms. Thompson's arrest?

A. I am not.

Q. In your experience, do large business clients generally want their internal data to be available to the public?

A. No.

Q. Do you have any reason to believe that Capital One wanted their data to be available to the public?

A. No.

Q. Did -- have you ever heard any suggestion, or has anyone at Capital One ever told you, that they wanted that to be available to the public?

A. No.

Q. Would that be unusual for a company with sensitive information?

A. Very.

Q. If a company actually wanted its information to be publicly available, would there be easier ways to do that than requiring someone to proxy through a firewall and take credentials?

A. Yes.

Q. In your experience, do large companies generally want roles that they have to be available to be assumed by members of the public?

A. No.

Q. Do you have any reason to believe that Capital One wanted its role to be generally available to the public?

A. No.

Q. You never heard any suggestion to that effect?

A. No.

Q. Would that be unusual in your experience?

A. Yes.

MR. FRIEDMAN: Thank you. I have no further questions.

THE COURT: Okay. Mr. Klein, any questions?

MR. KLEIN: Yes, Your Honor.

THE COURT: Oh, sure. Take as much time as you need.

MR. KLEIN: Just one second, Your Honor, while I set up.

I lost my pen.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good afternoon, Mr. Schuster. How are you?

A. I'm fine. Thank you.

Q. So I want to talk for a minute about some of the exhibits the prosecutor showed you.

First, I'd like to pull up Government Exhibit 103.

MR. KLEIN: Can you please publish that to the jury?

Is it -- can the jury see that?

THE COURT: No one can see that.

MR. KLEIN: One second, Your Honor.

THE COURT: Yeah. For a trial about high tech, we're not doing very well, are we?

(Off the record.)

MR. KLEIN: Your Honor, I'm going to put it up here on the -- oh, here we go.

THE COURT: Okay.

MR. KLEIN: That's actually 104.

Can we put up 103, please?

THE COURT: Do you have that in front of you?

THE WITNESS: Yeah.

Q. (By Mr. Klein) Mr. Schuster, can you see 103 now?

A. I can.

THE COURT: But the jury can't.

MR. KLEIN: How do I switch to this?

THE COURT: Do you want to help him with the camera?

(Off the record.)

MR. KLEIN: Apparently, I have the publish button. I didn't know that.

All right. So everyone can see this now just...

Q. (By Mr. Klein) Mr. Schuster, I want to talk to you for a moment about credentials, which you testified earlier about.

Just to clarify, credentials aren't a user name, are they?

A. Credentials are made up of a user name.

Q. But it's not a user name like when you log into your email; correct?

A. It -- that's one part of a credential is a user name that can be --

Q. Is there a password associated with a credential?

A. There is, typically, a password or a token or...

Q. A token, right.

So what is associated with a credential, let's start there?

A. So a credential would be a user name, which would be like your email, or an authentication process, which can be a password or a smart card or a token, another way to authenticate the user.

Q. Okay. And a credential is not always assigned to a specific person, is it?

A. Correct.

Q. And it can be shared; right?

A. Yes.

Q. And it can be even given -- the person who it's shared with can have the ability to share with other people; correct?

A. Yes. It's not the best practice.

Q. I'm not asking you if it's the best practice, but it can be shared with other people?

A. Yes.

Q. And it can be shared with other services?

A. Yes.

Q. And it can be even shared with third parties?

A. Yes.

Q. Okay. You testified about how authorized people can call up IMS. Do you recall that?

A. Yes.

Q. What is IMS again?

A. Instance Metadata Service.

Q. So that's what's on the bottom of Exhibit --

THE COURT: I think it was.

Q. (By Mr. Klein) -- 103?

A. It is.

Q. All right. And what is the Instance Metadata Service again?

A. It gives information about the instances that are running on the computer, on the hardware.

Q. Okay. So in addition to people, can't any services on an EC2 instance call up an IMS?

A. Yes.

Q. Okay. And can't those same services or software call up on behalf of others?

A. I'm sorry, ask that one more time.

Q. Can't software that's running on an EC2 instance call up the IMS on behalf of others, other computers?

A. Typically not.

Q. But can it?

A. If the role is configured as such, yes.

Q. Okay. So it can.

I'm going to turn to Exhibit 104 now. Hopefully, this will go smoother.

Does everyone see that? It should be published to everybody.

THE COURT: Yep.

Q. (By Mr. Klein) So I'm going to talk for a moment about S3 buckets.

S3 buckets, people store data, companies store data in the S3 bucket; correct?

A. Correct.

Q. And can you give me some examples of when companies -- or what companies share that data that's in their S3 buckets with other -- Amazon, AWS has a lot of customers, and do some of them share what's in their S3 buckets with others?

A. Yes.

Q. Okay. Is Netflix a customer?

A. They are.

Q. And do they share what's in their S3 bucket or S3 buckets?

A. I don't know details on Netflix.

Q. Do you know, does AWS have public libraries as customers?

A. Yes.

Q. Does it -- and do you know if they share their information that's in S3 buckets?

A. Again, I don't know the configuration of the libraries. If they store their books or their content in a bucket, they could share that information from the bucket. I just don't know the details.

Q. Do you know any AWS customers that do?

A. No.

Q. Don't know a single one?

A. I -- I do incident response, I don't do configuration of customers --

Q. Okay.

A. -- areas.

Q. But it's possible, and you're generally aware that they might do it?

A. It's absolutely possible, and that's one way to do it.

Q. Okay. Let's turn to Government Exhibit 105.

This is the firewall demonstrative. Do you see it?

A. I do.

Q. And do you remember talking about this with the prosecutor?

A. I do.

Q. So let's start at the beginning here.

Not every AWS customer has to have a web application firewall; right?

A. Correct.

Q. And not every AWS customer has to configure their web application firewall the same way; right?

A. Correct.

Q. In fact, they might not even want or need a web application firewall; right?

A. Correct.

Q. Okay. So setting aside for a moment how Capital One set up its web application firewall, other AWS clients might have wanted to set it up the way Capital One had set theirs up; correct?

A. I suppose, yes.

Q. Okay. And they might have done so for business reasons; correct?

A. Correct.

Q. Did you or any of your team at AWS help Capital One set up its web application firewall?

A. Not that I'm aware of.

Q. And as far as you know, they set it up themselves, Capital One?

A. As far as I know.

Q. Okay. Now I'm going to turn to Exhibit 106.

Do you recognize this exhibit?

A. I do.

Q. And this is the demonstrative that talks about the IAM Roles.

So for AWS customers, does AWS configure the IAM Roles?

A. No.

Q. Who does?

A. The customer.

Q. Okay. And the customer can configure the IAM Role however they want; right?

A. Correct.

Q. And AWS can't see how they configured unless they showed it to you; correct?

A. Correct.

Q. So unless the customer tells you how they've set it up, AWS does not know how it's configured or set up?

A. Correct.

Q. All right. So focusing in again on IAM Roles, they can be created for not just people; correct?

A. Correct.

Q. Who else can they be created for?

A. Computers, applications.

Q. Okay. And can they be created for people, computers, and applications outside of the company who is the client of AWS?

A. Yes, they can, but that's not --

Q. I'm just asking if they can.

A. Yes, they can.

Q. Okay. And can the AWS client who set up the IAM Roles, can they delegate access to other users?

A. Yes.

Q. Can they delegate access to other applications?

A. Yes.

Q. Can they delegate access to other services?

A. Yes.

Q. Okay. And can they grant access to third parties?

A. Yes.

Q. All right. Now I'm going to talk about web application firewalls again.

A. Okay.

Q. And bear with me because I'm an attorney and I'm still absorbing this, too.

So a web application firewall, it doesn't know why the person is issuing the command to it, does it?

A. It does not.

Q. Okay. And a person or service that finds an open web application firewall doesn't necessarily know why it's open, do they?

A. No.

Q. And I'm going to lay out what I understand the process to be. I'm going to ask you questions about it.

A. Okay.

Q. So the web application firewall, when it gets a request, it looks at that request; correct?

A. Yes.

Q. It then sees if the request complies with its configurations. Does that make sense?

A. Correct.

Q. And then the web application firewall decides whether the request is allowed?

A. Correct.

Q. And if it decides that the request is allowed, it allows the request to go forward?

A. Yes.

Q. Okay. So in the case of the web application firewall for Capital One, it was configured to allow the request we've been talking about with Ms. Thompson to go forward?

A. Well, the firewall wasn't exploited, the proxy, the reverse proxy --

Q. I'm just asking if the web -- focus on my question. The web application firewall configured the way Capital One had configured it, you've said you've looked at, was configured to let those requests go forward?

A. I have not looked at the configuration of their firewall. The request did not go through their firewall, it actually stopped at their firewall and used the proxy of the firewall to query the service.

Q. Let me phrase it in a different way, it was programmed to allow external requests, how about that?

A. Yes.

Q. Okay. So an outsider could make a request to that web application firewall?

A. Yes.

Q. And Ms. Thompson's request was identified as an external request; correct?

A. Yes.

Q. So Capital One's web application firewall operated as it was programmed, it identified an external request and allowed it to go forward?

A. It identified the external request. I can't speak to whether it went through the firewall or stopped at the firewall.

Q. But it was set up to permit external requests?

A. That's what firewalls do.

Q. Okay. So other AWS customers could configure their web application firewalls differently; right?

A. Yes.

Q. They can set up their firewalls not to allow certain types of external requests; correct?

A. Correct.

Q. In fact, they can set up their firewalls to deny requests from -- that come in through TOR; correct?

A. Correct.

Q. And often they do?

A. Correct.

Q. And that wasn't the case here with Capital One's web application firewall, was it?

A. I believe that's the case.

Q. Now, turning for a second --

MR. KLEIN: Can we go back to that exhibit? Did I unpublish by accident? Maybe I touched something.

Exhibit 106, please.

Q. (By Mr. Klein) Want to focus on the role for a moment. Do you see that here?

A. I do.

Q. The role -- and we talked about how a role -- what's a role again? Let's start there, just remind the jury.

A. A role is a way to describe a set of permissions that are allowed for a group of users or resources.

Q. Okay. And the role that Ms. Thompson was assigned -- because you've looked at this, you've looked at what she's alleged to have done here; right?

A. Yes.

Q. The role she was assigned permitted her to copy data; correct?

A. Ultimately, yes.

Q. I'm going to turn for a second now to Government Exhibit

952, that's the note you were discussing earlier.

A. Yes, sir.

MR. KLEIN: Can we publish that, please?

(Off the record.)

MR. KLEIN: Your Honor, I'll represent to Your Honor this is the same exhibit, it's just marked as Defense Exhibit 1100.

THE COURT: Okay. We can publish that to the jury. Go ahead. We're not going to admit it into evidence, but it's the same note.

MR. KLEIN: It's the same note.

Q. (By Mr. Klein) Do you see on your screen this note?

A. I do.

Q. Just happens to be in color this time?

A. I do.

THE COURT: Do you guys have it?

Okay. Great.

Q. (By Mr. Klein) You don't know who wrote this note, do you?

A. I do not.

Q. Is it possible that someone passed this along at Ms. Thompson's direction?

A. It's possible.

Q. And looking at the note exactly, you talked about the timestamp earlier?

A. Yes.

Q. Wouldn't that be essentially irrelevant because the server that Capital One -- or the configuration that was running was still set up the same?

A. I don't know whether it was still set up the same or not.

Q. Well, you talked about earlier this note was received in May?

A. Correct.

Q. And the incident that you talked about occurred in July; right?

A. The incident occurred in March.

Q. Well, when you --

A. Learned about it.

Q. -- said you learned about it and investigated it was in July; right?

A. Correct.

Q. So if the problem was the same in March as it was in July, does the timestamp matter -- the lack of a timestamp matter?

A. It absolutely matters because of the volume of data that would have to be gone through to determine what happened.

Q. But wouldn't the setup be the same if it was -- wasn't the setup the same?

A. No. We got notified in July about a data breach, information being public. And then we -- we did analysis with Capital One to understand how that data became available.

MR. KLEIN: Okay. Your Honor, may I approach with a new defense exhibit?

THE COURT: You can approach Victoria.

MR. KLEIN: Yes, that's what I meant.

(Off the record.)

MR. KLEIN: Your Honor, I provided a copy to the government already.

THE COURT: Okay.

THE CLERK: Defendant's Exhibit 1010 is marked.

MR. KLEIN: This would be Exhibit 1101, Defense Exhibit 1101.

THE CLERK: Okay.

THE COURT: Okay. 1101 is marked for identification.

Q. (By Mr. Klein) Mr. Schuster, do you see this exhibit yet?

A. Not yet.

Q. Okay.

A. I now see it.

Q. Do you see this exhibit, Mr. Schuster?

A. I do.

Q. Do you recognize it?

A. It's an email from me to Steve Schmidt.

Q. Who is Steve Schmidt?

A. Steve Schmidt at the time was the chief information security officer for AWS.

Q. Isn't it actually an email thread, though, there's more emails on here, if you look down?

A. It is an email thread, yes.

Q. But if you look at the second email, that's an email from you to other people at Amazon; is that right?

A. It is.

Q. Okay. And was it your practice to send emails as part of your work?

A. Always.

MR. KLEIN: And, Your Honor, the defense would like to offer this into evidence.

THE COURT: Any objection to 1101?

MR. FRIEDMAN: Your Honor, I think just because it's his practice to send emails doesn't make this qualify as a business records --

THE COURT: All I asked is if you have an objection.

MR. FRIEDMAN: Objection, yes.

THE COURT: I'm not going to admit 1101.

You can ask him about it.

MR. KLEIN: Sure.

Q. (By Mr. Klein) Do you recall in July of 2019 corresponding with Steve Schmidt about this incident?

A. I do.

Q. And do you recall discussing the note with others at Amazon?

A. Yes.

Q. And do you recall that you discussed the note, we're talking about the handwritten note, 1101, with people at Capital One?

A. I did not discuss it with them directly.

Q. Do you recall that it was brought up in a meeting with them?

A. This would have been my team.

Q. I'm asking if you recall it was brought up in a meeting?

A. Not me directly, no, sir.

Q. Do you recall that it was brought up in a meeting with other people on your team?

A. Yes.

Q. Okay. And do you recall that the note was discussed with your team at that time in the context of the breach they were looking at then?

A. We were trying to determine if the note was associated at all.

Q. Okay. So the note was part of your discussions or part of your team's discussions at the time?

A. It was.

Q. And Capital One was aware of the note?

A. Yes, because we passed it to them.

Q. And at a meeting during this time, it was brought up?

A. I'm assuming so, yes.

Q. Okay. Let me talk to you for a moment about Amazon's responsible disclosure exhibit, which is Exhibit 952, I believe.

Let me make sure.

I'm sorry, 954.

MR. KLEIN: Your Honor, this is not loaded into the system, but I'm going to talk about it.

Q. (By Mr. Klein:) So you talked for a moment about the responsibility disclosure system Amazon has in place?

A. Yes.

Q. Do you know if that was the program in place in 2019, the one you read from?

A. I don't know whether we had a formal program in 2019, but we had been dealing with responsible disclosure my entire time at Amazon.

Q. But the thing you talked about, you don't know if it was in place in 2019, do you?

THE COURT: The one you were shown.

Q. (By Mr. Klein) The one you were shown --

A. Right, right.

Q. Right.

A. I don't know the timestamp on that, it may have changed since then, between then and now.

Q. Okay. So that might not necessarily be the program that was in place in 2019?

A. Because there's no timestamp on it; that's correct.

MR. KLEIN: Okay. One second, Your Honor.

THE COURT: Okay.

(Off the record.)

MR. KLEIN: Last couple questions here.

THE WITNESS: Sure.

Q. (By Mr. Klein) When someone -- you talked about responsible disclosure for a while. You're not in charge of setting up this program, though, are you?

A. The formal program, no, but I'm responsible for implementing it.

Q. Okay. And when someone makes a responsible disclosure, does it have to be perfect or can there be minor inconsistencies in what they say versus what you learned later when you look at it?

A. When someone comes to us with responsible disclosure, I have a team that reaches out to the customer or the people who have reported it and try to work with them to make sure that I completely understand the issue.

Q. Sometimes responsible disclosures are anonymous, though, aren't they?

A. Sometimes they are.

Q. And sometimes they're incomplete, aren't they?

A. They are.

MR. KLEIN: Nothing further.

THE COURT: Mr. Friedman, any more questions for Mr. Schuster?

MR. FRIEDMAN: Yes, Your Honor.

REDIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Mr. Schuster, defense counsel asked a question that -- whether roles could be configured for outsiders. Do you remember that question?

A. I do.

Q. And you said yes and started to provide an explanation?

A. I did.

Q. And defense counsel said no, I just wanted yes or no. What explanation did you want to provide?

A. I wanted to provide the explanation that that is not a standard practice.

If customers want the broad audience, the Internet, to interface with them, they would not assign roles, they would make the information public; they would make the service public without assigned roles.

Q. Okay. You testified that Capital One -- you were asked whether other customers might want this configuration, right, whether that --

A. I was.

Q. Okay. Was Amazon concerned enough that they wouldn't, that it took steps?

A. We did.

Q. Okay. Why was that?

A. Because it was an error that caused enough significant risk that we were worried about copycats and other companies making similar errors.

Q. Okay. Did you form an opinion -- when you were investigating or learning about the breach that happened in this case, did you form an opinion about the attacker's sophistication and degree of knowledge and computer expertise?

MR. KLEIN: Objection, Your Honor. Calls for speculation.

THE COURT: Well, asking for an opinion --

UNIDENTIFIED SPEAKER: Or an expert opinion.

THE COURT: -- yeah. I'm going to sustain the objection, but if you rephrase the question maybe.

Q. (By Mr. Friedman) Okay. Did you believe -- did you see some of the code used and the methodology used for this attack?

A. I did not see the code, but I know it was available and we looked --

Q. Did you understand the methodology?

A. I did.

Q. Okay. Did it appear to you to be fairly complex?

MR. KLEIN: Objection, Your Honor. Lack of foundation.

THE COURT: Overruled.

You can answer, just from your lay opinion.

A. Okay. My opinion was each step was not overly sophisticated; brought together in a series of steps that got all the way through, was a unique and novel approach.

Q. (By Mr. Friedman:) Okay. Let's look at Exhibit 952, the note, if we could?

I believe you testified that this did not accurately describe the methodology for the attack?

A. That's the note; right?

Q. It is the note. I'm sorry. It should appear.

THE COURT: I like their color version better.

MR. KLEIN: We're happy to let the government use that version.

THE COURT: There it is.

MR. FRIEDMAN: Thank you.

THE COURT: The black and white one.

Q. (By Mr. Friedman) Does this accurately describe what happened in this case?

A. No.

Q. You were asked whether it was possible that Ms. Thompson was the person that asked for this to be communicated?

A. I was asked.

Q. If she was the person who asked or directed or wrote this note, would you expect it accurately to describe what was done?

MR. KLEIN: Objection, Your Honor. Calls for speculation.

THE COURT: Yeah, it does, but go ahead, you can answer.

A. It does not accurately represent. What was accomplished was the download of millions of financial records. This indicates it was just access to security credentials.

Q. (By Mr. Friedman) Okay. And it misdescribes the proxy that was used; correct?

A. And it misdescribes the proxy.

Q. Would you expect the person who had conducted the attack to be able to accurately describe what was done?

A. I would hope, yes.

MR. FRIEDMAN: Thank you. I have no further questions.

THE COURT: Okay. I think you're done.

Let me ask you one question, though, because I'm always interested in the language. You go back a long ways, I'm not saying you're old or anything, but...

THE WITNESS: Careful, Judge.

THE COURT: But why did they -- why did we settle on cloud versus sky or atmosphere or ocean or swamp or something?

THE WITNESS: That's actually a really good question.

Going back to the very, very beginning of the Internet when people would describe network, architectures, or how computers would set up, in the middle always started with a cloud.

THE COURT: Okay.

THE WITNESS: It always started with this -- there's this amorphous thing called the Internet, but what we really care about is how we connect up to the Internet. And so since we always use the cloud, then we started thinking about companies able to move things off of their prem -- off of their premise, into a shared area or whatever, cloud just seemed a natural --

THE COURT: Okay. That makes sense. Appreciate it. Thank you.

THE WITNESS: You're welcome.

THE COURT: All right. You're excused. Thank you very much.

We'll do the government's next witness.

MS. MANCA: Your Honor, the government calls --

MR. KLEIN: Your Honor, sorry, one second, we would like him to be subject to recall.

THE COURT: Of course, you know, we can bring any witness back at a later time.

MR. FRIEDMAN: The only thing I would say is Mr. Schuster lives on the East Coast and is probably headed to the airport.

THE COURT: Yeah, but if we need to, we'll bring him back. We'll put him up at the Spheres.

Yeah. Thanks very much.

THE WITNESS: Thank you.

THE COURT: So one of the reasons I'm a lawyer is when I was at Brandeis University in 1970, I took a computer science class. This is an old mainframe computer. You know, this is a long time ago.

And I started doing something where I started erasing all the memory banks in the computer. And bells started going off, and lights flashing, and they ran to where I was and said leave and never come back. So that's how I'm a lawyer and a judge.

Okay. The government's called Kat Valentine; correct?

MS. MANCA: Yes.

THE COURT: Ms. Valentine, please come into this open area of the courtroom here. And raise your right hand and my clerk will swear you in.

That's good.

KRISTEN VALENTINE,
having been first duly sworn, testified as follows:

THE CLERK: Okay. Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Sure. It's Kristen Valentine. Valentine like the holiday, V-a-l-e-n-t-i-n-e.

THE COURT: And Kat is your nickname?

THE WITNESS: And Kat is my nickname. Even my mother calls me that.

THE COURT: All right.

THE CLERK: Should we get a spelling on the first name, Your Honor?

THE COURT: No, no, we're good, but give her a cup just in case she wants some water, too.

Do you have one up there?

THE WITNESS: Yes.

THE COURT: And since we're doing nicknames: Jess, do you want to ask your questions?

DIRECT EXAMINATION

BY MS. MANCA:

Q. Good afternoon, Ms. Valentine. I'll give you a second with your water.

A. Thank you.

Q. So where did you grow up?

A. Miami, Florida.

Q. And where were you living in 2019?

A. Antioch, California.

Q. How did you get from Miami Beach to Antioch, California?

A. Antioch is in the Bay Area, which is tech Mecca, right, and that's what I do for a living. So kind of worked my way west and stopped at a few places along the way.

Q. How did you get involved in technology?

A. I -- my father gave me my first computer at age six and my first phone line at age seven, so like a separate phone line from them.

Q. And then once you, you know, got older, growing up into a grown-up, what did you do to learn technology?

A. Well, as a teenager, I attended 2600 meetings, technology enthusiasts hacking community kind of thing.

And then at 18 I got my first tech support job at -- and from there I was a NOC analyst or network operations center analyst. Then I was a Cisco -- like a Cisco VoIP engineer for a little while. And then I pivoted into information security versus a vulnerability researcher; and then doing compliance, which is much more general, and as an auditor for the payment card industry at first, but other stuff later.

Q. So you're self-taught with all your technology skills?

A. Yeah. And I had a friend of mine teach me Slackware when I was 17, but, yeah, mostly.

Q. And what do you do now?

A. Right now I'm an independent consultant. I consult a lot of Bay Area companies, big companies, small startups, things like that, on SOC2, HIPAA, PCI compliance, that sort of thing.

Q. What do you help those companies do?

A. I help them understand the data security standards for each compliance regiment. Mostly, I act as a translator for folks that are engineers, like so I can identify what about their current architecture doesn't meet standards, what they would need to improve, gap assessments, things like that, as well as teach like the lawyers of those organizations what these rules mean and how it can affect them risk assessment-wise.

THE COURT: So when you say SOC 2, what does that stand for?

THE WITNESS: Sorry. I'm like so nervous, I'm vomiting.

THE COURT: Oh, no.

THE WITNESS: I don't remember what SOC actually stands for --

THE COURT: Okay.

THE WITNESS: -- but --

THE COURT: But it's like a regulation --

THE WITNESS: It is, yeah.

THE COURT: -- that they have to comply with.

HIPAA is the health information --

THE WITNESS: Health Information Privacy and Portability Act.

THE COURT: So you're advising companies that may be way up here on tech and computer, hey, you've got to meet these regulations and make sure you're not violating anything.

THE WITNESS: Yeah.

THE COURT: Okay.

THE WITNESS: Yeah, because usually these different compliance regiments have rules or data security standards and things like that.

THE COURT: Sure.

THE WITNESS: And a lot of companies think that they're doing a lot of the right things, so I usually come in, identify gaps --

THE COURT: Okay.

THE WITNESS: -- in compliance and then help them fix it.

THE COURT: Just relax. You know, we're just talking. We're just having a conversation. It's no big deal, okay?

THE WITNESS: Okay.

THE COURT: Okay. Yeah. Go ahead, Ms. Manca.

Q. (By Ms. Manca) I'm going to take you back to 2019, the summer of 2019. Did you have a Twitter account around that time?

A. Yes.

Q. Was it a public account or a private account?

A. It was a public account.

Q. Do you remember what your Twitter name or Twitter handle was at that time?

A. At that time it was K.J. Valentine, basically my name.

Q. And anyone could message you if you have a public Twitter account?

A. Yeah.

Q. What information did you have about yourself in your Twitter profile?

A. A profile picture, my name, Kat Valentine, and probably -- I don't remember exactly what I had in the pro -- in the profile, but you can put a bio, and it probably just had my interests, like hack freak, artist, that kind of thing.

Q. In -- you know, around the summer of 2019, do you remember just generally what kind of topics you were posting about?

A. Yeah. So I'd actually had my account -- kind of some important context. I had my Twitter account since 2009, but I didn't really use it all that much until I -- I was working a startup, quit my job, and decided that I wanted to do something a little more artistic than technical that particular summer. So I made -- I designed hacker shoes, and it's three shoes, and, uhm -- that kind of celebrated the culture a little bit. And I knew that a lot of Infosec people and hacker people were on Twitter, and that's where everybody kind of went to. So even though it wasn't my norm, I went on with the designs and said, hey, if -- does anyone even like these mockups? But if so, like I'll make 'em, and if not, cool, but it gained some traction and attention.

And so that's what I was doing on Twitter in the summer.

Q. So it kind of increased your Twitter profile through posting these shoes?

A. Yeah.

Q. And if someone had looked at the kind of things you were posting about other than shoes, would it have been sort of technical information, security type topics?

A. Yeah, it would have been. Yeah.

Q. Around that time, you know, June 2019, did you receive any messages on Twitter that are relevant to this case?

A. Yes.

Q. What kind of messages were they, public or private?

A. They were DMs or direct messages, so they were private.

Q. And what information did you have about the person or account who messaged you?

A. A profile pic, a name that the user can set, as well as the -- as well as the user name on Twitter.

Q. Is this a person that you had ever chatted with online before?

A. No.

Q. Did you have any idea what -- who this person was?

A. No.

Q. And over what length of time did you receive these messages?

A. About four days.

MS. MANCA: Agent, could you call up Exhibit 203?

Q. (By Ms. Manca) Now, we've previously gone over this exhibit. Do you recognize Exhibit 203 as a fair and correct copy of the Twitter messages you received?

A. Yes.

Q. Okay. And how did you preserve those messages once you saw them?

A. I didn't preserve them once I saw 'em, that came a little later. But I basically made screenshots either on my computer or on my phone, I don't remember which one.

Q. And is Exhibit 203 the screenshots that you took?

A. Yes.

MS. MANCA: Your Honor, we move to admit Exhibit 203.

MR. KLEIN: No objection, Your Honor.

THE COURT: Which ones are you going to use with this witness?

MS. MANCA: 203, 204, 201 -- sorry, out of order, so 201, 202, 203, 204, and 209.

THE COURT: Any objection to any of those, Mr. Hamoudi?

MR. HAMOUDI: Let me check, Your Honor, one quick second.

THE COURT: Sure.

MR. HAMOUDI: No objection to those, Your Honor.

THE COURT: Okay. They're all admitted into evidence.

And you can just post them and publish 'em right away.

(Government Exhibits 201, 202, 203, 204, 209 admitted.)

MS. MANCA: Thank you, Your Honor.

So can we go ahead and publish Exhibit 203?

Q. (By Ms. Manca) So you were testifying about these messages that you received. Can you tell us which part of the messages are the person's Twitter handle?

A. Yeah. The one with the @ symbol is the Twitter user name handle.

Q. So what's in the upper left-hand corner?

A. Erratic. That would be a display name that the user could set for themselves.

Q. And what about -- there's a photograph of a woman. Did you -- can you tell us what that photograph is?

A. It's a photograph of a woman.

Q. Did you recognize the person by sight?

A. No.

Q. And what's the name for that person on a Twitter profile?

A. An Avatar or profile pic.

Q. Can you tell us how you reviewed these messages as they came in?

A. Yeah. Because I didn't really use Twitter, I didn't have it like set up to notify me immediately when I got like messages and stuff, it was more I'd check it once a day, especially since there was a lot of traffic coming in from the shoes that I posted. So I didn't like live-check it or anything, like I would just check messages once a day. I mostly hung out on Facebook.

Q. So we're going to be going through some of these lines, you know, one at a time. But is that the way that you were reviewing and receiving these messages, one line at a time?

A. No. No. It would be like chunked, basically. So it would be like I'd, you know, hop on, and there was like a wall of messages or wall of texts waiting.

MS. MANCA: Agent, can you highlight the line, I'm gonna dox myself.

Q. (By Ms. Manca) So we highlighted this line, I'm going to dox myself. Did you understand what it meant to dox?

A. Yeah. I'm going to drop information on myself.

Q. And does dox typically have a public -- or, I'm sorry, a positive or a negative connotation in technology?

A. It typically has a negative connotation, but it's pretty neutral -- used neutrally here.

Q. What makes you say that it's used neutrally?

A. The negative -- the negative context usually for the word "dox" is usually a person, A, is dropping information like a name, you know, a real name and a phone number, an address, things like that, I mean, on person B, when person B wouldn't want that kind of information dropped online, so that's why it has a negative connotation normally. But somebody dropping information on themselves, consider it kind of neutral; right.

MS. MANCA: Yeah.

Q. (By Ms. Manca) can we pull out of that and go to -- there's a link in here to a GitHub Gist. Did you understand at the time you received these messages what a GitHub Gist was?

A. I know -- I knew what GitHub was, but I didn't know what a gist was at the time.

Q. Okay.

A. Namely because I work in compliance, it's kind of the softer side of Infosec, whereas GitHub is where a lot of coders hang out, and I'm not a coder.

Q. Can you tell us what your understanding was of GitHub?

A. It's a -- it's a code -- it's a platform that allows coders to have repositories of code. That allows other coders to take a look at the author's code and make -- make changes to it, proposed changes. And then the original author can approve those things, and it goes into -- and that goes -- gets merged into their repository.

Q. Do you now know what a gist is?

A. Yeah.

Q. And what is it?

A. It's similar to a paste bin where you can just put command line text there quickly for somebody else to review, or maybe even a couple-line script, something that doesn't need like collaboration and change management, you can just paste it there.

MS. MANCA: Agent, can you go to the next page?

I'm sorry, same exhibit, but page down.

There we go.

Would you mind highlighting that first tweet?

Q. (By Ms. Manca) So this statement, jacked, and then the link, all available S3 buckets, certs.

When you read that, did you understand what that meant?

A. Yeah. I understood jacked to mean like stole. All available S3 buckets, S3 buckets are offering on AWS. It's a storage solution. And then certs I assumed was like an -- encryption certs.

MS. MANCA: Okay. That's good, thank you.

Q. (By Ms. Manca:) Did you click on the link, do you remember?

A. No, not that I can recall.

Q. Why would you not have clicked on the link at the time?

A. The person messaging me is a stranger. I just kind of automatically, working Infosec, don't click on links that people send my way. It's just not good practice. Even though I knew at the time it was probably a safe link to click on because the preview here says GitHub.com and that's a pretty trusted website, but I just probably didn't.

Q. And the last line says, Are we there yet. Did you understand what that meant?

A. I didn't at the time. When looking back at it later and kind of actually like for real analyzing the messages, I thought -- I think it means like have you figured it out yet, like have you clicked on the link and figured out what's going on here.

MS. MANCA: Can you scroll down to page 5?

Q. (By Ms. Manca) So once again, these are messages you're reading all at the same time; correct?

A. Yeah.

Q. What do you think when you come to this message about dropping Capital One's dox and admitting it, wanting to distribute those buckets, SSNs with full name and date of birth? Are you processing that?

A. Uhm, it's kind of -- it's like a -- at the time I'm just kind of reading everything all at once. And it was such an outlandish claim that I -- you know, I really was -- there's a lot of people online that make a lot of outlandish claims, so I just was more so thinking about like who is this, why are they -- what are they trying to tell me, and can I get a crumb of context. Like that's more what I was thinking about, as opposed to actually digesting that, if that makes sense.

Q. And so there's a response in blue.

MS. MANCA: Agent, can you highlight that response?

Q. (By Ms. Manca) Who wrote that?

A. I wrote that.

Q. And what does it mean, I gotta ask, this Claire in?

A. So Claire is a friend of mine, and she plays a lot of pranks. She hops on Twitter quite a bit with SOC accounts, taking on different personas, basically.

Q. What's a SOC account?

A. It's a -- like an alternative account that doesn't represent you, you know. So I thought at first it was this girl Claire because the messages were outlandish, kind of unbelievable. And the language, like Claire speaks that way. So I thought it was Claire, right, so that's why I'm asking that.

MS. MANCA: Okay. Can we keep going down?

Can you scroll down to the next page?

Thank you.

Q. (By Ms. Manca) And do you recognize these messages as messages that you reviewed?

A. Yeah. I think it's like the next day or something at this point, but, yeah, I do.

MS. MANCA: Can you keep scrolling down?

Keep scrolling.

Okay. Agent, can you highlight the bottom, the last tech tweet and the response.

Thanks very much.

Q. (By Ms. Manca) So is this the end of your Twitter correspondence?

A. Yeah.

Q. What does lamer with a three mean?

A. It's a very '90s hacker thing, insult to throw somebody's way. I wasn't responding to the messages, so she was just calling me lame.

Q. And then what did you write in responses?

A. Or not a snitch. Go snitch on yourself, FBI.gov, big homie, which is a very '90s hacker thing to say as well. Basically, whatever you're claiming, I don't want anything to do with. And you know, if it's -- whether it's true or not, but, basically, I was just living my life at this point, and then I blocked her.

Q. Is that why it says you can no longer send messages to this person?

A. Yeah.

Q. So you go about your life at this point after having blocked her on Twitter?

A. Yeah.

Q. Do you think anything more about these messages at that point?

A. No. Like I said, there's outlandish claims made on the Internet all the time, so didn't really believe it, didn't click on the links, so had no reason to take it seriously.

Q. And at some point you go back and you revisit these messages; is that right?

A. Yeah, that's right.

Q. Without getting into any conversations you had with other people, can you tell us about how you went back and revisited those messages?

A. Yeah. So about two weeks later, it was July 4th, and I remember that because July 4th a friend of mine -- an old associate of mine sent me a Twitter DM saying, hey, take a look at this tweet. And so it was like a public tweet. And she's like a bit of a gossip and things like that. So I took a look at the tweet and I said, hey, give me a crumb of context what this is about. She did.

And I noticed that -- I said, you know -- I said to my associate, I said, wait, the user name looks really familiar to me, like it looks familiar, and the picture looks familiar.

So I navigated to the profile of the user name and it says, you know, that you had blocked this person. So I said, oh, okay, I must have interacted with them, because I completely forgot at this point. So then I searched my DMs and said, oh, it's this conversation, it's this, okay.

Q. And again, without getting into anything anyone else said, do those messages that you're talking about have anything to do with these messages that we're looking at right now? Was it the same topic or a different topic?

A. I'm sorry?

Q. The one that your friend was looking at and saying, oh, these tweets over here, was that something else entirely?

A. It was something else entirely. It was a totally different topic, but she just happened to show me this tweet. I looked at the user name, said, oh, wait, I remember that, and then went back to the DMs.

Q. And at that point, you know, my understanding is that you and your friend had some conversation about what was happening with the tweets. And again, without getting into the substance of that conversation, did you eventually click on that GitHub link?

A. I did, yeah.

MS. MANCA: And Exhibit 204 has been admitted in evidence. Can we publish Exhibit 204?

Q. (By Ms. Manca) Okay. Do you recognize this as the content of the link that you clicked on?

A. Yeah. Yes. Yes.

Q. Okay. And understanding that it took you some time to look at this document and you revisited it on other occasions, what stood out to you about this?

A. If you -- if you could scroll?

MS. MANCA: Could you scroll to the next page.

THE WITNESS: Okay. Stop.

MS. MANCA: Agent, could you expand some of the...

Thank you.

A. Yeah. So at that time, me and my associate were both looking at this page. And the thing that stood out were the bucket names, you know. At first, you know, we're basically just -- because it's -- it was a pretty long list of bucket names, so -- and the thing that stood out about the bucket names was card prod, you know, it would be like Canada card prod 1 or -- and that sort of stuff. Working in tech, prod means production, so it's live data, and then card usually means cardholder data.

Q. (By Ms. Manca:) So what did you think that these files or folders were showing?

A. I thought that it was a list of the different S3 buckets. And I think at one point my associate and I even commented that one says Cap One or something like this. And, uhm, we both came to the conclusion that this was legitimate.

MS. MANCA: And so if we could scroll to the very last page of this document, which is, I think, 47.

Agent, can you expand that last comment?

Thank you.

Q. (By Ms. Manca) Did you get to the end of this GitHub Gist, what I've expanded on the screen right now?

A. Yeah.

Q. And is this part of the gist with all of those buckets or is this something else?

A. Yeah. This is a -- this is a command.

Q. And when you looked at this command, did you understand what it did?

A. I got the gist. Did a little Googling on sync to make sure it meant downloading, basically, and then concluded that probably these S3 buckets were downloaded.

Q. And which was the command that made you think it had been downloaded?

A. Sync.

Q. S-y-n-c?

A. Yeah.

Q. So once that you realized that these buckets had probably been downloaded, did you make a decision to report this to someone?

A. Not right away, but eventually, yeah.

Q. Okay. What made you decide to report it?

A. So my associate, kind of a second voice of reason at the time, started saying we should report this, you know, like this is live, I'm going to go ahead and notify customers -- my customers, things like that, that there's probably something really bad going on here. She told me that she would look into it.

About an hour later, she said, never mind, don't report it. And I thought that was suspicious, so then I looked into it, and then spent the next two weeks kind of mulling over what this would mean. Went back over the text -- the direct messages again as well because now I'm paying attention. And, you know, one of 'em said that Ms. Thompson was going to disseminate the information, or whoever was on the other side of it.

Q. At the time, did you know who it was?

A. No.

Q. Okay.

A. Uhm, I mean, I assumed from the GitHub link where it has her name that it was -- that it was Ms. Thompson, but I still didn't know who that person was, like as a person, so still a stranger.

And it was -- but, basically, the thinking at the time was, all right, well, if the contents of this gist are correct and indicative of a breach, then maybe everything else that was in the DM is true, too, such as I'm going to disseminate this information to a scammer.

And working in this field and the sheer amount of buckets, it took me two weeks to come to the conclusion that I had to report it.

The only entity that could determine that this really was a breach was Cap One, so I reported it there.

Q. How did you figure out where to report it to Capital One?

A. I Googled Capital One disclosure.

Q. Once you Googled that, did you find a place to -- or information about reporting responsible disclosures?

A. Yeah. There was a disclosure page. It had rules of engagement and what they're not looking for in reports and things of that nature. And then at the bottom of the page, there was an email address.

MS. MANCA: Agent, could you pull up Exhibit 209?

Thank you.

Q. (By Ms. Manca) Do you recognize this as -- this is from way back, right, but do you recognize this as the web page that you reviewed?

A. Yeah.

Q. And you mentioned that it has responsible disclosure program guidelines?

A. Yeah, it has --

Q. You called them something else, rules of engagement?

A. Rules of engagement, yeah.

Q. Okay. And then Out of Scope Vulnerabilities, what are those?

A. Out of scope -- it looked like -- so every -- every disclosure program is usually -- it's different, it's usually tailored to the organization, and there's like -- they're generally the same, but they have little differences here and there. So out of scope is what that particular company considers out of scope, they're not interested in, et cetera, or they don't want you to do. So, for example, like DDoSing their servers or something, yeah.

Q. And is there an email address at the very bottom?

A. Yeah.

Q. And is that the address that you emailed?

A. Yep.

Q. I'm going to call your attention, then, to Exhibit 201, if we could publish that.

Is this the email that you sent to that email address?

A. Yes.

Q. Okay. And what link were you sending them?

A. So there were -- in total in the DMs, I think there were like four or five links. And it referenced other companies, but this one is the one with the Capital One says three buckets. So

I was just sending them the link relevant to them.

Q. Okay. And how quickly did you get a response back from someone in Capital One?

A. The next day.

MS. MANCA: Okay. And if you could call up Exhibit 202.

Q. (By Ms. Manca) Is this a copy of the email exchange that you had with Capital One after they responded to you?

A. Yeah.

Q. And who is Kate Torelli?

A. She's an employee at Capital One. My understanding, I could be wrong on this, is that she's like an incident response manager. But I could be wrong, I don't know.

Q. And she's the one you spoke to?

A. On the phone, yeah.

Q. Okay. And so how did you talk to Kate Torelli, which methods of communication did you use?

A. At first, she just emailed me back, as you can see at the bottom there, saying we're looking into this, we have a couple of questions.

I think I responded back with like a, yeah, I have time this afternoon. I gave my phone number, I think.

Either way, we ended up exchanging information; connecting on the phone, sometime in the afternoon in my afternoon PSD, so...

Q. And you ended up sending some additional information, what additional information did you send?

A. It was relevant to our phone call because, basically, you know, how the conversation started was she was basically like, okay, so this is a private gist, like how did you get this? And I was like, well, starts with shoes, like -- and, uhm, basically, you know, had to explain to her like, I don't know, I just got these -- these DMs on Twitter containing the links, told her the story a little bit. And, uhm, then she said, hey, can I have screenshots of what you got in the DMs? I said, sure, no problem.

So what's here, I think -- I think this is the email where I attached like screenshots.

MS. MANCA: Can you scroll down a few pages?

A. Yeah. So, uhm, those are the screenshots of the -- of the DMs as requested.

And then, uhm, she also wanted the links. I mean, it's not like she can click on the picture and get to the link, so I included that as well.

Q. (By Ms. Manca) You mentioned something about a private gist. I don't think I asked you what a private gist is.

A. Basically, a private gist, it's not searchable on Google. So they wouldn't have like caught this in a Google Search or something like that. You need to have the direct link in order to look at the contents of it.

Q. And that's what this link was?

A. Yeah.

Q. Was a private gist, okay.

So after you sent this information, did Capital One offer to pay you for this information?

A. No -- well, not at first, but eventually they did.

Basically, how that went is during our first phone call, I asked -- because I noticed on the web -- responsible disclosure web page, I noticed that it said that they don't pay for -- you know, it's not like a bug bounty kind of thing, but a ton of companies do pay for it, so I thought it was weird that a financial institution wouldn't, you know, like pay for it, right. So I was like, you guys really not pay for it, pay for tips and stuff like that? And, you know, Kate was like, yeah, no, we don't. We have this internal political thing where our Infosec department wants to do that, but, you know -- but, you know, higher-ups don't want to pay for that kind of stuff. So I said, nah, I understand. I worked at a company like that, too, we would give away crappy T-shirts and we would sometimes do that. You know, sometimes we would mess that up and not even send the T-shirts, so I get it. And so we were just kind of bantering like that.

After a couple of phone calls, though, I noticed that Kate started saying, hey, so I'm -- you know, I'm working on getting you a reward. And I said, your page said you don't reward, I don't really need one, I don't want one, you know, I'm good. But she kept insisting on it and, uhm, she said, you know, that internally at Cap One and politically this was a really good example of why they should pay rewards. So she wanted -- so she wanted to give -- she kind of insisted. And I told her I don't -- I don't want to be paid for this, I don't feel right about it. If you need to do that for your own political whatever within Cap One, just go ahead and donate the money to the EFF and the Diana Initiative, and that's what happened there.

Q. Did you personally accept any money, then, for this?

A. No.

THE COURT: EFF is electronic?

THE WITNESS: Electronic Frontier Foundation, yeah.

THE COURT: And they are just a sort of a good -- not government, but look for ways to help people on the Internet and in electronics?

THE WITNESS: Yeah. Basically, it was my two favorite charities.

THE COURT: What was the other one?

THE WITNESS: Diana Initiative. It's basically a -- more inclusion of women in computing.

THE COURT: Okay. Okay. Great.

Ms. Manca, are you almost done?

MS. MANCA: Last question, yes, Your Honor.

THE COURT: Okay. Great.

Q. (By Ms. Manca) And Exhibit 203, those text messages that we looked at, are those the only text messages -- or, I'm sorry, I'm saying text, Twitter.

So Exhibit 203, are those the only Twitter messages that you exchanged with the handle or user name Erratic?

A. Yeah.

Q. Okay. Did you have any other conversations with that person and in any other forum?

A. Not to my knowledge, no.

MS. MANCA: Okay. No further questions. Thank you.

THE COURT: Okay. So we're going to do cross-examination, but we're going to take a break first because we've been doing this for an hour and a half.

THE WITNESS: Okay.

THE COURT: And when we take a break, it's complicated. So Victoria is going the take the jurors down to 14. And just stay where you are while we move the jurors out.

And everyone please stay in their seats.

Go ahead, Victoria. Thank you.

Leave your notepads and pens on your chairs.

(Off the record.)

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: When we come back, Mr. Hamoudi, who is a really great guy, is going to ask you some questions.

THE WITNESS: Okay.

THE COURT: And then we'll let you go, okay?

THE WITNESS: All right. Thank you.

THE COURT: Thanks for coming up.

I think it's safe to go out now.

(Court in recess 3:03 p.m. to 3:24 p.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Okay. Your cross-examination of Ms. Valentine, Mr. Hamoudi?

CROSS-EXAMINATION

BY MR. HAMOUDI:

Q. Good afternoon, Ms. Valentine. You thought this was a cry for help, didn't you?

A. I did later, yes.

Q. Your Twitter profile, it had a link to your LinkedIn profile?

A. No, but I have a pretty unique name, so it's easy to search on LinkedIn.

Q. So your LinkedIn profile, I want to talk to you about your professional background.

A. Sure, yeah.

Q. Okay. All right. And just for references, this profile is used for professional networking and career development?

A. Yes.

Q. Okay. And in there, you have significant amount of experience in providing strategic, architectural, audit, operational security strategies across many industries, correct?

A. Yes.

Q. Including credit card compliance companies, correct?

A. Yeah. PCI is how I got my start in information security when I pivoted from general tech, yes.

Q. And you've been responsible for both security and compliance of many well-known cloud providers?

A. Yes, yeah.

Q. Credit card providers?

A. Not credit card providers, no.

Q. Or banks?

A. I've done consulting for Fintech. But at the time that this happened, I had not worked for a bank. I've since done a gig for a bank, yes.

Q. And payment providers?

A. Payment providers, yes.

Q. Security platforms?

A. Yes.

Q. Okay. And you'd done this for over ten years when you got these tweets?

A. When I got the tweets? Yes.

Q. Okay. And you also have -- you have, like, a YouTube channel, or you talk about security compliance, you're active in it, or a podcast?

A. I was on the Security Weekly podcast after this event, yes.

Q. And it sounds like you're passionate about computers.

A. I've been doing it since I was six, so, yeah.

Q. Yeah. Is it, then, a challenge for a person such as yourself to find professional mobility in this industry?

A. I think when first starting out, yes, but once you have a little something under your belt, it becomes easier.

Q. Could you imagine that it would be the same for someone who may be transgender?

A. I imagine it would be much more difficult.

Q. Can you talk about that a little bit?

MR. FRIEDMAN: Objection; relevance.

THE COURT: I'll allow a little bit. Go ahead.

A. Repeat the question. Talk a little bit about?

Q. (By Mr. Hamoudi) The challenges that somebody who's transgender would experience to get involved in the tech community.

A. It's a really hateful world.

Q. Yeah.

A. And tech -- I would say tech can be kind of toxic sometimes. It's toxic for women, people of color, and especially transgender people.

Q. And I saw that you're a member of InfraGard.

A. I was a member of InfraGard.

Q. You were?
A. Yes.
Q. And that's a partnership between the FBI --
A. And private industry.
Q. -- and private industry and for protection of U.S. critical infrastructure?
A. Yeah, that's right.
Q. And that was also on your LinkedIn profile?
A. That was.
Q. I want to talk a little bit about the process of getting the DM messages and, sort of, what unfolded.
A. Sure.
Q. At some point, you went and looked at the gist link that you saw, the computer information, correct?
A. Yeah, not the first pass, but two weeks later.
Q. Two weeks later?
A. Yeah.
Q. I want to bring up something on the gist link, and I'm going to show you another previously admitted exhibit, and see if you see any parallels, any similarities.
A. Okay.
Q. Okay?

This is the note, and this is the gist link. Take a look at the note. Do you see that note?
A. Yeah, I do.

Q. And then look above, and do you see the gist link, the gist file?

A. Yes.

Q. Do you see a similarity with that IP address?

A. Yeah. The first thing that's screams out is it's the same IP address.

Q. And it also talks about proxy? Those are the same things?

MS. MANCA: Objection, Your Honor; mischaracterizes the exhibit.

THE COURT: The exhibit speaks for itself.

You can answer the question.

THE WITNESS: Repeat the question.

Q. (By Mr. Hamoudi) Do you see the word "proxy" in both of them?

A. Yes, I do.

Q. Okay. Great.

You Googled the Capital One responsible disclosure on Google; is that --

A. Yeah, exactly.

Q. And then you went to their website?

A. Yes.

Q. And then you sent an email to them, correct?

A. That's right.

Q. Okay.

MR. HAMOUDI: Marked for identification Defense

Exhibit 1010, and can you just zoom up to the top so she can see it?

Q. (By Mr. Hamoudi) Do you recognize this email?

A. Yes.

Q. Is this the response you got from Capital One?

A. That's the first response I got, yes. It's is an autoresponder.

MR. HAMOUDI: Move to admit Defense Exhibit 1010.

MS. MANCA: No objection.

THE COURT: 1010 is admitted into evidence and can be published.

(Defense Exhibit 1010 admitted.)

Q. (By Mr. Hamoudi) So let's walk through what this is saying. What does the line say?

A. "Please submit an official report through HackerOne." At the time -- I know that, at the time, Capital One was moving from this general mailbox to hackerone. They'd explained that to me in the first phone call.

Q. Did you talk to them about this -- did you go to hackerone and set up an account?

A. I did, and I submitted a report as well, like the autoresponder said to do, yeah.

Q. Okay. So Defense Exhibit 1011 --

MR. HAMOUDI: Marked for identification. Do not publish, please.

Q. (By Mr. Hamoudi) Do you recognize this?

A. It's been three years, but, yeah, it looks pretty self-explanatory, yes.

Q. Okay.

MR. HAMOUDI: Offering 1011.

MS. MANCA: No objection.

THE COURT: 1011 is admitted and can be published.

(Defense Exhibit 1011 admitted.)

Q. (By Mr. Hamoudi) This is the Capital One vulnerable disclosure program within the website hackerone, correct?

A. Yeah, hackerone is a platform that a bunch of companies will post a page like this on, yes.

Q. And when was the program launched? If you can look, it says right at the bottom.

A. Oh.

THE COURT: Well, according to the document.

MR. HAMOUDI: According to the document.

THE COURT: She doesn't know.

THE WITNESS: I actually do know something about it.

THE COURT: Oh, good. Go ahead.

A. On the document, it says April 2019 --

Q. (By Mr. Hamoudi) Okay. But maybe for additional context: The reason Cap One -- the Kate Torelli lady over at Cap One did tell me that they were just moving over to hackerone.

THE COURT: That was in July when you talked to her?

THE WITNESS: Yeah.

A. They were just moving over and kind of smoothing out bugs. Spinning up a program on hackerone does take a little time and effort, yeah.

Q. (By Mr. Hamoudi) So they were all on this website, and then in July, when you spoke to her, they were talking about moving it to somewhere else?

A. No.

THE COURT: No.

MR. HAMOUDI: Sorry. I may have misheard.

THE COURT: What she said is this may say it transitioned in April, but it actually took them a few months to get to hackerone.

MR. HAMOUDI: Okay.

Q. (By Mr. Hamoudi) So --

A. So there was somebody staffing the mailbox as well, and that's why Kate Torelli, the next day, emailed me, even though I submitted something through hackerone, as well as the original email. And HackerOne, actually, closed the report, too, initially.

Q. Not everybody uses responsible disclosure programs, correct?

A. That's right, not everybody does.

Q. And there was, actually, a struggle between yourself and somebody else about whether to use this program, correct? About whether to report it to Capital One, there was a disagreement?

A. Oh, yes.

Q. Okay. And reporting isn't easy?

A. Reporting is -- it's a lot easier now than it was, but it's still not -- it's still not crisp across the industry, that's right.

Q. And some people in the hacking community are scared to disclose, correct?

A. I know I was.

Q. Yeah. And some people don't trust companies?

A. That's right.

Q. Some people don't trust the government?

A. That's right.

Q. And can you explain, what does it mean that HackerOne closed a report, when you just said that?

A. Sure.

So for context, HackerOne is a platform where security researchers and companies -- it's kind of the middleman for that stuff.

One of the services that HackerOne offers, which, I believe, Cap One utilized, is that HackerOne's own analysts will take a look at reports that come in first, kind of to filter the noise out a little bit. They initially closed the report, and Kate -- but Capital One was still monitoring that email box, even though they had an autoresponder up, and tell HackerOne to reopen the report and that it was legitimate. And they, actually, came back with a whole lot of argument for me on it. So it was very difficult through HackerOne, an established third-party bug bounty platform.

Q. It sounds kind of complicated.

A. It was.

Q. So going back to the messages --

MR. HAMOUDI: If we can bring up --

Q. (By Mr. Hamoudi) You said -- on direct testimony, you said you had looked at the particular account, card prod, card prod account?

A. Yeah. In the gist, there is a lot of S3 buckets that have "card prod" in the name, yes.

Q. But you didn't look inside the actual file to see what was inside there?

A. You couldn't.

Q. No, but you didn't go and try to access --

A. No, I didn't.

Q. Okay. So is the reason why you know card prod account might contain sensitive data is because you have some experience in the credit card industry?

A. Yeah. "Prod" commonly means "production," and "card" means cardholder data. It's very -- yeah, very common.

Q. Just one last question.

A. Sure.

Q. No, I think that's it.

MR. HAMOUDI: I have no more questions. Thank you.

THE COURT: Usually when a lawyer says "one last question," there's five. This time there was zero. That really threw me for a loop.

Anything further, Ms. Manca?

MS. MANCA: Yes, one question.

THE COURT: Let's see how many we end up with here.

REDIRECT EXAMINATION

BY MS. MANCA:

Q. Was one of the factors that made this difficult for you the fact that you were reporting someone else's activity?

A. Absolutely.

Q. If it had been a situation where you were just reporting a vulnerability that you had just seen in the world, would that have been easier?

A. Like, emotionally? Yeah.

MS. MANCA: No further questions. Thank you.

MR. HAMOUDI: One second, Your Honor. Ms. Thompson is speaking to me.

RECROSS-EXAMINATION

BY MR. HAMOUDI:

Q. Even if you were reporting on behalf of somebody else, isn't it still difficult?

THE COURT: I don't understand the premise of the question.

Q. (By Mr. Hamoudi) You said that your reporting on somebody, it still presents difficulties just reporting, in and of itself?

A. Just generally reporting a vulnerability?

Q. Yes.

A. Yes.

MR. HAMOUDI: Thank you.

THE COURT: Thanks, Ms. Valentine. You are excused.

THE WITNESS: Awesome.

THE COURT: I really appreciate your testimony.

Mr. Friedman, we'll start with one more witness.

MR. FRIEDMAN: Sure. The government calls Michael Fisk.

THE COURT: Mr. Fisk, if you'll come into this open area of the courtroom here and raise your right hand, my clerk will swear you in.

MICHAEL FISK,
having been first duly sworn, testified as follows:

THE CLERK: Please state your name for the record, and spell your last name for the court reporter.

THE WITNESS: Michael Fisk, F-i-s-k.

THE COURT: Thank you, Mr. Fisk. Go ahead, Mr. Friedman.

MR. FRIEDMAN: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good afternoon, Mr. Fisk.

A. Good afternoon.

Q. How are you?

A. I'm okay.

Q. You work in cyber security; is that correct?

A. I do.

Q. How long have you done that?

A. Nearly 30 years.

Q. Where did you start working in cyber security?

A. I worked my way through college as a systems administrator at the university, and that was the first place that I worked some computer security incidents and cases, but then throughout my career after that.

Q. Your first job, did that involve cyber security work?

A. Yes, part of the job, yes.

Q. Where was that?

A. New Mexico Tech.

Q. Okay. It was your first real job, after college, involving cyber security?

A. Yes. After college, I went to Los Alamos National Lab.

Q. Okay. And what is Los Alamos National Lab?

A. It is a federally funded research and development center for the United States Government that does work for a number of agencies.

Q. Mr. Fisk, you have one of the weaknesses I have, which is you talk really fast.

A. Sorry.

Q. I bet the court reporter would really appreciate if we both slow down.

A. I'll do my best.

Q. What did you do at Los Alamos?

A. Well, I worked there for 25 years. I worked on computer security for much of that; network security. I was on the -- founding member of the first security incident response team; led the Laboratory Cyber R&D programs for multiple government agencies.

Q. What is a security incident response team?

A. That is the team that deals with security alerts, investigates, and determines how to respond to them.

Q. At some point did you take on a managerial role in cyber security?

A. Yeah. At various points I led all of the network security and security operations teams, and subsequently, later on, became the chief information officer of the laboratory for four years, which included being the senior security executive.

Q. When did you become the chief information officer at Los Alamos?

A. 2014.

Q. And how long did you stay at Los Alamos?

A. I left in 2018.

Q. Where did you go?

A. Capital One.

Q. What job did you take at Capital One?

A. I took a role as deputy chief information security officer and vice president.

Q. And in general terms, what are your responsibilities? Well, when I say "what are," are you still at Capital One?

A. No, I left earlier this year.

Q. Where did you go then?

A. I now work for Meta.

Q. Are you also involved in cyber security there?

A. Yes. I'm still a deputy chief information security officer and head of security engineering for financial technologies products.

Q. And Meta is the company we all love that used to be Facebook?

A. Correct.

Q. Is it fair to say you were at Capital One as the deputy CISO from 2018 through early 2022?

A. Correct.

Q. In general terms, what were your responsibilities at Capital One?

A. It varied, but it included cyber architecture, mergers and acquisition, our line of business, information security officers, a product management function that we built to interact with shared technology teams that were implementing security requirements.

Q. Did you have a role or responsibilities related to a breach that happened in 2019?

A. I did.

Q. And what was your role with respect to that breach?

A. As soon as I became alerted to an investigation, it sounded like something that needed as much attention as we could give it, so I went down to the security operations center, and, except for a little bit of time to sleep, didn't come back out for a couple of weeks working on the investigation.

Q. Did you have a technical role with respect to that investigation?

A. Yeah. I, essentially, led the technical investigation of forensic analysis and collection of the root cause analysis as it unfolded.

Q. We're going to come to that, obviously, in a few minutes. But can you tell us, in general terms, what is Capital One Financial Corporation?

A. It is a holding company for the banks, multiple lines of business and business entities.

Q. And what lines of business does the bank have?

A. It has a banking business, an auto-loans business, probably most recognizably, a credit-card-issuer business.

Q. Why do you say "most recognizably"?

A. I think it is the number three issuer in the country, or was recently, and there is a lot of ads you may have seen.

Q. And mail we've received, maybe?

A. Perhaps.

Q. The data that was taken in this breach, from which part of Capital One's business was that?

A. From the card line of business.

Q. The credit-card-issuing portion?

A. Correct.

Q. I want to ask you about Capital One's computer architecture, generally.

I assume there was a time when Capital One had its own servers and data farms; is that correct?

A. Yes, and data centers.

Q. And when did that change?

A. In the twenty-teens, the company made a strategic decision to move primarily to the public cloud environment, and, specifically, AWS.

Q. In the twenty-teens; can you say, roughly, when in that period?

A. I think a lot of decision was around 2014 or 2015. It was before I started.

Q. By 2019, when the breach happened, how far along had that migration gone?

A. It was largely complete. We hadn't finished shutting down the last data centers but had moved the vast majority of applications and workloads to the public cloud.

Q. Did Capital One have a cyber security organization even before this movement?

A. Yes.

Q. And it continued after, I assume?

A. Yes.

Q. What is that cyber security department or division or organization called?

A. In 2019 and today, it's just called the Cyber Organization, and previous to that, it was the Information Security Risk Management Organization.

Q. Is it okay if we go with "Cyber Organization"?

A. That works.

Q. How big was the Cyber Organization in 2019?

A. It was about 700 people, I think.

Q. What was the annual budget of it; do you know?

A. It was a couple hundred million for that team, which doesn't include security functions, you know, built into the other parts of the shared technology environment that I mentioned earlier.

Q. And am I understanding correctly that the general information technology, or whoever maintains the computers and makes sure that happens, that's a different thing than this team you're talking about?

A. Right. There's a much larger technology organization.

Q. So the $200 million and the 700 employees were all devoted to security?

A. Correct, full-time security.

Q. Is it possible to break out and sort of tell us the general categories in which the Cyber Organization's work fell?

A. Yeah. There's a lot of areas that go into a well-rounded security program. I sort of think of it in terms of preventive, and then sort of detect-and-response thing. So on the preventive side --

Q. Let's go one type of measure, single one at a time.

The preventive side, so --

A. Yeah, so preventive, that includes like identity and access management, things like how people authenticate with multifactor authentication.

Q. Is another word for that the credentials that are required to prove -- that's not a word, it's a phrase -- but is another description of that the credentials required to prove that you are the person that you say or purport to be?

A. Essentially, yes.

Q. Okay. Why does the Cyber Organization insist of that kind of function?

A. Well, setting and managing standards and expectations around access control and access-control technologies is sort of one of the more fundamental first things you do in terms of controlling access to data.

Q. Can you explain, in broad terms, why that's important?

A. Well, you wouldn't want data, particularly through customer private information, to be accessible to people that don't need to access it, so you restrict the access to people who are authenticated and authorized.

Q. And does part of that include deciding what data each person is allowed access to?

A. Yeah. In the field, there's a discipline known as access management or role management in the process for granting and reviewing access.

Q. Are you familiar with something called the principle of least privilege?

A. I am.

Q. What is that?

A. Essentially, as the name says, that you would like to give the least amount of access to a person or a computer in order to, you know, perform its job or function, but not do anything else that's unnecessary.

Q. Was that one of the things the Cyber Organization tried to accomplish?

A. Yeah. It's a principle, by the name, which is something that organizations are always striving for, and certainly was included in our approach to things. It's usually something that's not ever fully achieved.

Q. A goal, at least?

A. Yeah.

Q. Are there other techniques or approaches that the Cyber Organization used in order to try and achieve cyber security?

A. Yeah, a number of them. Network security, firewalls, intrusion detection, vulnerability scanning and penetration testing.

Q. Can you tell us what vulnerability scanning is?

A. Yes. It's continually testing all of the computers in your environment to see if they have any known vulnerabilities.

Q. Did Capital One do that?

A. Yes.

Q. Did it do it itself, or did it hire outside contractors to come in and do that?

A. We used one of the leading companies and tool providers who provide software that we ran and used as a service.

Q. Okay. What company is that?

A. Qualus.

Q. And how regularly did that happen?

A. It was continuous. I think we had an expectation that every asset was scanned at least every three days.

Q. Are you familiar with something called pen testing?

A. Yes.

Q. Was that also a measure that Capital One used?

A. Yes.

Q. What is pen testing?

A. It's short for "penetration testing," and it is typically having an expert, skilled person or a team manually attempt to break into a system from the outside, but sometimes from the inside.

Q. Did Capital One have internal employees that performed pen testing?

A. Some, and then also outside firms.

Q. Okay. What firms did you hire to do that?

A. I think one was SRA, Security Research Associates, or something like that, and I don't recall the name of the other one.

Q. How regularly would pen testing be conducted?

A. They were engaged most of the year, but, you know, sort of making the rounds around different things to test.

Q. Okay. But was it regular and repeated?

A. Yes.

Q. Are you familiar with something called a "red team"?

A. Yes.

Q. What is a red team?

A. A red team is another form of expert testing where you try to break into things. That is a little bit more goal oriented, achieving an objective compared to pen testing, but, otherwise, somewhat similar.

Q. Do you know where the name red team comes from?

A. I believe it comes from red team, blue team sort of military exercises where you're going to want to have your offensive and defensive team spar against each other and make each other better.

Q. Did Capital One have an internal red team, or did it hire contractors to do that?

A. Internal.

Q. Okay. Was that team constantly working, attempting to break in?

A. Yes.

Q. Were all of the people that we've talked about -- the pen testers, the company engaged in scanning, the red team -- were all those people or organizations that Capital One had asked or contracted to do that?

A. Yes.

Q. Okay. To your knowledge, were there random teams out there saying, Let's try Capital One and call them if it works?

A. No, that wouldn't fall into the normal notion of a red team.

Q. And why is that?

A. Because a red team is sort of an authorized exercise usually with some pretty clear ground rules about what the target is and what the team can and can't do.

Q. Okay. Did Capital One, basically, authorize the scanners, the pen testers, and the red team --

A. Yes.

Q. -- to do what they did?

A. Yes.

Q. Everything we've talked about, I think you mentioned that part of what the Cyber Organization did was preventive measures; is that correct?

A. Yes.

Q. Is everything we've talked about so far preventative?

A. Yeah, I'd put them in that bin.

Q. And is there another group or category of work that the Cyber Organization was engaged in?

A. Yes. There's also a detection-and-response role.

Q. Let's just go one by one.

What did Capital One Cyber Organization do for detection and response?

A. So that includes running intrusion-detection services, monitoring them for security alerts, having a 24 by 7 operations team that would investigate those alerts and respond to them.

Q. Okay. What is an intrusion-detection system or team?

A. So it's a class of commercial product that, again, you can buy from vendors or services that watch traffic, typically on a network or on a computer, looking for malicious activity and creating an alert if it sees something suspicious.

Q. Did Capital One have that either internally or contracted?

A. Yes.

Q. Are you familiar with something called "GuardDuty"?

A. Yes.

Q. What is GuardDuty?

A. It's an Amazon product that is, essentially, a cloud intrusion-detection service.

Q. Did Capital One contract or purchase that product?

A. Yes, we used it.

Q. You also mentioned "incident response." What is incident response?

A. So you have an operations team that assesses alerts that come out of various detection tools, and then if something is determined to be potentially successful, and if it merits further investigation and response, and that gets into an incident response.

Q. And then are you familiar with something called "responsible disclosure"?

A. Yes.

Q. What is responsible disclosure?

A. It's a common thing that's done in the industry, which most companies and government agencies and the like, will publish a means by which a security researcher who identifies a vulnerability can responsibly disclose that vulnerability to the owning entity so that it can be fixed in the public interest.

Q. And Capital One had a program at the time?

A. Yes.

Q. Did the responsible disclosure program authorize people to engage in white hat hacking, trying to penetrate Capital One's systems?

A. No.

Q. Was there any specific authorization, or was it just an address you could call if you learned of a vulnerability?

A. Essentially, the latter.

Q. Okay.

Now I'm going to turn to the breach.

The account or buckets that were penetrated, did they relate to a particular area of Capital One's business?

A. Yeah, we, as I said, moved most of our environment to the AWS infrastructure, and AWS resources are grouped into what AWS calls "accounts," which is more like sort of a billing account than a person-logging-in account. And so Capital One had several hundred accounts, and there was one, in particular, that was a card-production account that was involved.

Q. Okay. Do you recall the name of that account?

A. Yeah. It was COF-card-prod. That's our stock ticker symbol. "Card" for the business line, and "prod" is a production environment.

Q. COF is the ticker symbol that means Capital One Financial?

A. Yes.

Q. And what part of Capital One's business used this account?

A. It was the card-issuing line of business.

Q. What types of employees or people had access to or used data in the account?

A. So it was used by, you know, people who are supporting customers who call up with a problem, for example, through specific applications that those agents would use to access your account and help you. It's used by business analysts who are determining who to make credit offers to and at what line of credit and sort of otherwise analyzing the financial data.

It's used to handle financial transactions when you actually make a purchase with a Capital One credit card, for example. And it's also used for cards that don't necessarily have a Capital One logo on it but from some of our partner firms; store cards, for example, as they're commonly called.

Q. Can you explain what a partner or a store card is?

A. Yeah. So retailers will enter into agreements with credit card issuers to issue a card that's branded for that store, like a Walmart or a Bass Pro.

Q. So it is a credit card that says "Walmart," but really it's Capital One doing the banking behind it?

A. Correct.

Q. What kind of decision-making was the information within that account used for?

A. Like I said, it's used, you know, up front to decide what kind of credit limit to offer to customers, to give them an offer for a credit card. The mail that you alluded to earlier.

Q. Okay. So is that sometimes called acquisitioning?

A. Yeah. Acquisitioning is acquiring customer accounts.

Q. Okay. Apart from that, what was it used for?

A. It's made for further sort of decisioning on credit limits, where people get credit-limit changes over time, and that's included as well.

Q. Okay. Are you familiar with -- it seems like we're turning every noun into a verb.

Are you familiar with transactioning?

A. Yes.

Q. Was it used for that?

A. Yeah. Like I said, you make your credit card purchase, and, you know, at the end of the month it shows up on a statement, right from the bank, and all that transaction information ends up flowing through our systems.

Q. And was it also used on the back end, you know, in terms of cards that were overdue or cards that were going to be closed?

A. Yes. Certainly to generate any sort of claim, yeah, notice that people haven't paid bills or followed through, that sort of thing.

Q. The entire life cycle of a credit card, basically?

A. Yes.

Q. In order to access or use that data, how would a Capital One employee or a Capital One machine or server do that?

A. So most employees would go through an application interface. Often it's browser-based application interface, where you log in, typically, with multifactor authentication, and then the application determines what customer data you need to see to perform the role that you have in the function that the application provides.

Q. Was access to that ever just generally, at least intentionally, generally open to the public, to anyone that wanted to access that data?

A. No. There were, you know, websites where a customer can log in and get to see your data after logging in with multifactor authentication, typically. And in the end, you're seeing some data from that account, but through multiple layers of authentication security.

Q. Would all access, whether it's employee or customer, require some form of authentication?

A. Yes.

Q. And when you talk about "authentication," what do you mean by that?

A. Typically, it boils down to having some sort of key or credential that represents you and, as a result, the permissions that you, as a person or a computer, have, and presenting that credential to a service to access data.

Q. Okay. I'm sorry. I may have just missed that.

Would that involve both an account identity or a role identity and a security credential?

A. Yeah. Like a user name and a password with the keys for computers that don't necessarily use passwords in the way that you and I would, but they have, again, both for the identity and a key, yes.

Q. Okay. When we were talking a moment ago, I think we talked about internal Capital One employees and users and servers, but you also mentioned that members of the public would sometimes be able to access a portion of that data; is that correct?

A. Yes, their own data.

Q. Would a member of the public be able to access anything but their own data?

A. No.

Q. Would even that access require credentials or some form of authentication?

A. Yes.

Q. And what would that require?

A. So you log in with a user name and password, and for many operations, particularly if it's not coming from a device that we're used to seeing it come from, it will require a two-factor authentication as well.

MR. FRIEDMAN: Your Honor, if the court is looking to break, this is a good time, or I can keep going.

THE COURT: I thought we might go a little longer, but how much more do you have?

MR. FRIEDMAN: Probably another hour.

THE COURT: We'll go ahead and break now.

MR. FRIEDMAN: Thank you.

THE COURT: You can come back tomorrow, I assume.

THE WITNESS: Yes.

THE COURT: And then we'll ask you about Area 51, and Los Alamos, too.

We're pretty much on schedule to do the witnesses that we were planning to do. We didn't quite finish the last one today.

But please don't do any research about the case. Don't try to see what those hacking sneakers are that Ms. Valentine was talking about. Just be in tomorrow at about 8:45 so we can get started promptly at 9:00. Tomorrow, we have a judges meeting at noon, so we're really going to need to stop on time. And then at four o'clock tomorrow, we have an investiture for one of our magistrate judges, Kate Vaughan, who became a United States magistrate judge during the pandemic, and we've had to postpone the ceremony for so long.

Leave your notepads and pens on the chair. We'll see you tomorrow at 9:00 for a full day of trial.

Thank you.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Do you have --

MR. FRIEDMAN: Two things: One, when the court said we're on schedule, I just wanted to let you know, the schedule we turned in, we listed people under the day we thought they would start. So I think we are on schedule, but we expect some of those to fall into the next day.

THE COURT: Yeah, you have a couple possibilities. Tuesday of next week.

MR. FRIEDMAN: Correct, right.

And then the second thing was, with this witness there's going to be one exhibit that has some sensitive information. It's sensitive Capital One information. And so our intent was, ultimately, when we file it, to file a redacted version and ask the court to publish that. We have yet to file that one. We would like to show it the Court, opposing counsel, and jury, but turn off the screen to the gallery, and I'll identify it at the time.

THE COURT: It is a business record that's particularly sensitive to Capital One?

MR. FRIEDMAN: It is a lot of logs that, basically, show commands that are being issued and exactly what happened at different times.

THE COURT: Sure. You can do that.

MR. FRIEDMAN: Thank you, Your Honor.

THE COURT: Anything you want to bring to my attention?

MR. HAMOUDI: No, Your Honor.

THE COURT: Okay. We'll be adjourned. Thank you.

(Proceedings adjourned at 4:07 p.m.)

CERTIFICATE

I, Marci E.C. Chatelain, CCR, RPR, RMR, CRR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 8th day of June, 2022.

/s/ Marci E.C. Chatelain

Marci E.C. Chatelain, CCR, RPR, RMR, CRR
Federal Court Reporter